Turin

NETWORKS

Adit 3000 Series and Multi-Service Router (MSR) Card

GUI REFERENCE MANUAL

Part Number: 770-0169 BB
Product Release: Adit 3000 Series - 1.6
MSR Card - 2.0
April 2008

Copyright 2008 Turin Networks Inc. All rights reserved.

The information presented in this manual is subject to change without notice and does not represent a commitment on the part of Turin Networks Inc. The hardware and software described herein are furnished under a license or non-disclosure agreement. The hardware, software, and manual may be used or copied only in accordance with the terms of this agreement. It is against the law to reproduce, transmit, transcribe, store in a retrieval system, or translate into any medium - electronic, mechanical, magnetic, optical, chemical, manual, or otherwise - any part of this manual or software supplied with the Adit 3000 series or MSR products for any purpose other than the purchaser’s personal use without the express written permission of Turin Networks Inc.

The Turin Networks logo and Adit are registered trademarks of Turin Networks Inc. All other brand or product names are trademarks or registration trademarks of their respective companies or organizations.

Corporate Contact Information:

Turin Networks
1415 North McDowell Blvd.
Petaluma, CA 94954
Phone: +1-707-665-4400
Fax: +1-707-793-4935
www.TurinNetworks.com

Customer Support:
E-mail: tech-support@TurinNetworks.com
Phone: 800-786-9929 or 303-218-5655

Supporting Software Versions:

Adit 3104 - Release 1.6

Adit 3200 - Release 1.6

Adit 3500 - Release 1.6

Multi-Service Router (MSR) Card - Release 2.0

PREFACE

Safety Information

CAUTION! **WHEN USING YOUR TELEPHONE EQUIPMENT, BASIC SAFETY PRECAUTIONS SHOULD ALWAYS BE FOLLOWED TO REDUCE THE RISK OF FIRE, ELECTRIC SHOCK AND INJURY TO PERSONS, INCLUDING THE FOLLOWING:**

- Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.
- Refer to the installation section of this manual for a safe and proper installation procedure. All wiring external to this equipment should follow the current provision of the National Electrical Code

NOTE: For Safety and Compliance information for the Multi-Service Router (MSR) card and Adit 600 platform, please refer to the *Adit 600 User Manual*.

Notices

This manual contains important information and warnings that must be followed to ensure safe operation of the equipment.

DANGER! **A *DANGER* NOTICE INDICATES THE PRESENCE OF A HAZARD THAT CAN OR WILL CAUSE DEATH OR SEVERE PERSONAL INJURY IF THE HAZARD IS NOT AVOIDED.**

CAUTION! **A *CAUTION* NOTICE INDICATES THE POSSIBILITY OF INTERRUPTING NETWORK SERVICE IF THE HAZARD IS NOT AVOIDED.**

WARNING! **A *WARNING* NOTICE INDICATES THE POSSIBILITY OF EQUIPMENT DAMAGE IF THE HAZARD IS NOT AVOIDED.**

NOTE: A *Note* indicates information to help you understand how to perform a procedure or how the system works. Notes should be read before performing the required action.

Table of Contents

Preface

1 Web Based Management

2 Advanced

3 Network Connections

4 Security

5 System Monitoring

6 Voice Over IP

Glossary

Index

CHAPTER 1

Web Based Management

This Reference Manual covers the web-based Graphical User Interface (GUI) for the following products:

- Adit 3000 series (Adit 3104, Adit 3200, and Adit 3500)
- Multi-Service Router (MSR) Card (a service card for the Adit 600 platform)

These products are generically referred to as "the Adit" in this manual.

The web-based GUI provides a user-friendly interface for setup of the unit. This interface provides a Quick Setup option for the unit, as well as specific features for advanced setup.

NOTE: Throughout this manual, examples primarily reflect the Adit 3000 series. Where differences exist for the MSR card, these differences are noted.

In this Chapter

Overview of Supported Products

The following products have different hardware configurations, as well as optional features that can be purchased (for example, a VPN software keyed feature), therefore there are many possibilities for window options. For the most of the examples in this manual, the Adit 3500 is shown, as the majority of features are available on this product.

Adit 3104 IP Business Gateway

The Adit 3104 IP Business Gateway incorporates VoIP capabilities with a high-performance router. It supports a single T1 or Fast Ethernet WAN port, four-port Ethernet switch, stateful firewall, intrusion detection, and terminates up to 24 voice lines of VoIP.

The Adit 3104 creates a secure partition between external public network access while enabling remote users to securely connect to their businesses.

Adit 3200 Business Router

The Adit 3200 collapses multiple network entities - a high-performance router, managed switch, and stateful firewall - into one compact device. By providing a T1 termination port and an Ethernet port, it provides the ability to upgrade bandwidth without the need to replace hardware. The Adit 3200’s advanced VoIP-aware routing engine provides wire-speed throughput even when all security features have been enabled.

Adit 3500 Trunk Gateway

The Adit 3500 integrates the features of a trunk gateway, high-performance router, and stateful firewall, with flexible WAN options. It replaces multiple elements at the customer premises that typically provide routing, security, and trunk gateway functions, offering a powerful blend of speed, security, data, and voice. Additionally, a 4-FXS option provides connectivity for analog fax and modems.

This single platform offers scalability and high-performance for Internet and IP access, LAN-to-LAN connectivity over private and public networks, and VoIP PBX trunk service applications.

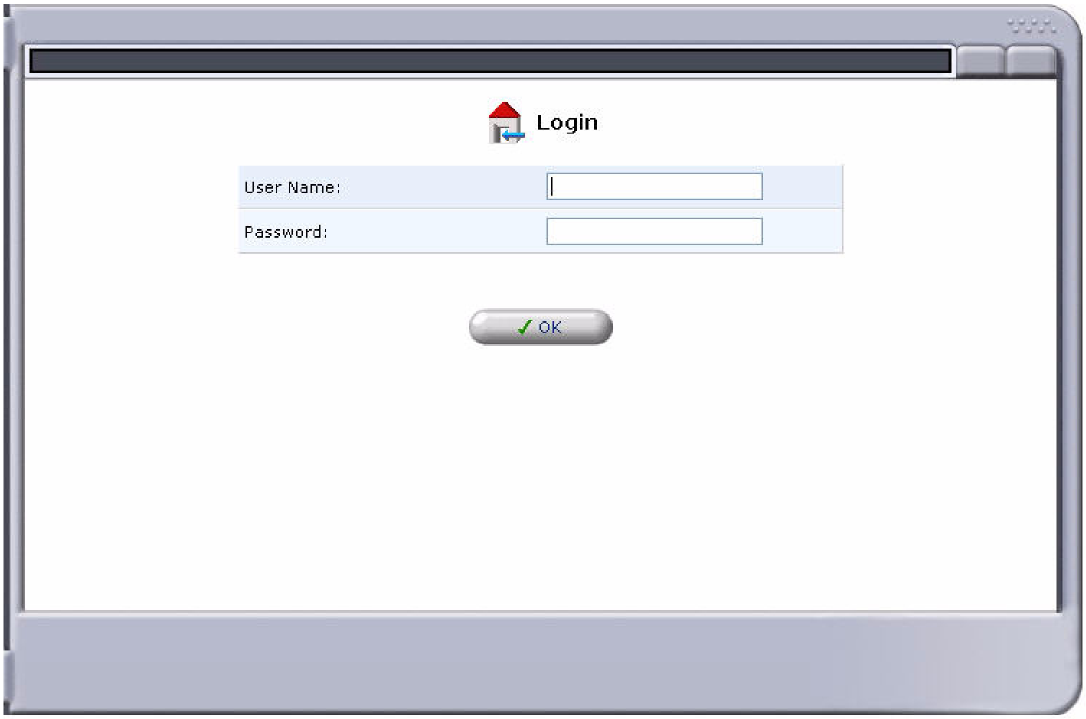
Multi-Service Router (MSR) Card (for the Adit 600 Platform)

The Multi-Service Router (MSR) card for the Adit 600 integrates the features of a trunk gateway, high-performance IPSec VPN-capable router, and stateful firewall with flexible WAN options. It replaces multiple elements at the customer premises that typically provide routing, security, and trunk gateway functions – offering a powerful blend of speed, security, data, and voice. When integrated into the Adit 600, the MSR card offers scalability and high performance for Internet and IP access, LAN-to-LAN connectivity over private and public networks, and VoIP PBX trunk service applications

Accessing the GUI

NOTE: The following instructions assume that you have connected your PC to the Ethernet port on the Adit 3000 (3104, 3200, or 3500) or MSR card. For additional connection options, see the *User Manual* for your product.

1. Launch a web browser on your PC from the same LAN as the Adit 3000 or MSR.
2. Enter the Adit 3000 or MSR card's IP address or name in the address bar.
   The default IP address is **http://192.168.1.1**. The **Login** screen appears.



Login

User Name:

Password:

3. Log in to the unit by entering the user name and password.
   - The default user name is **admin**
   - The default password is **admin 123**

NOTE: For security purposes, the user name and password should be changed from the default settings after the initial login. See *Editing a User* on page 2-67 for information on modifying user names and passwords.

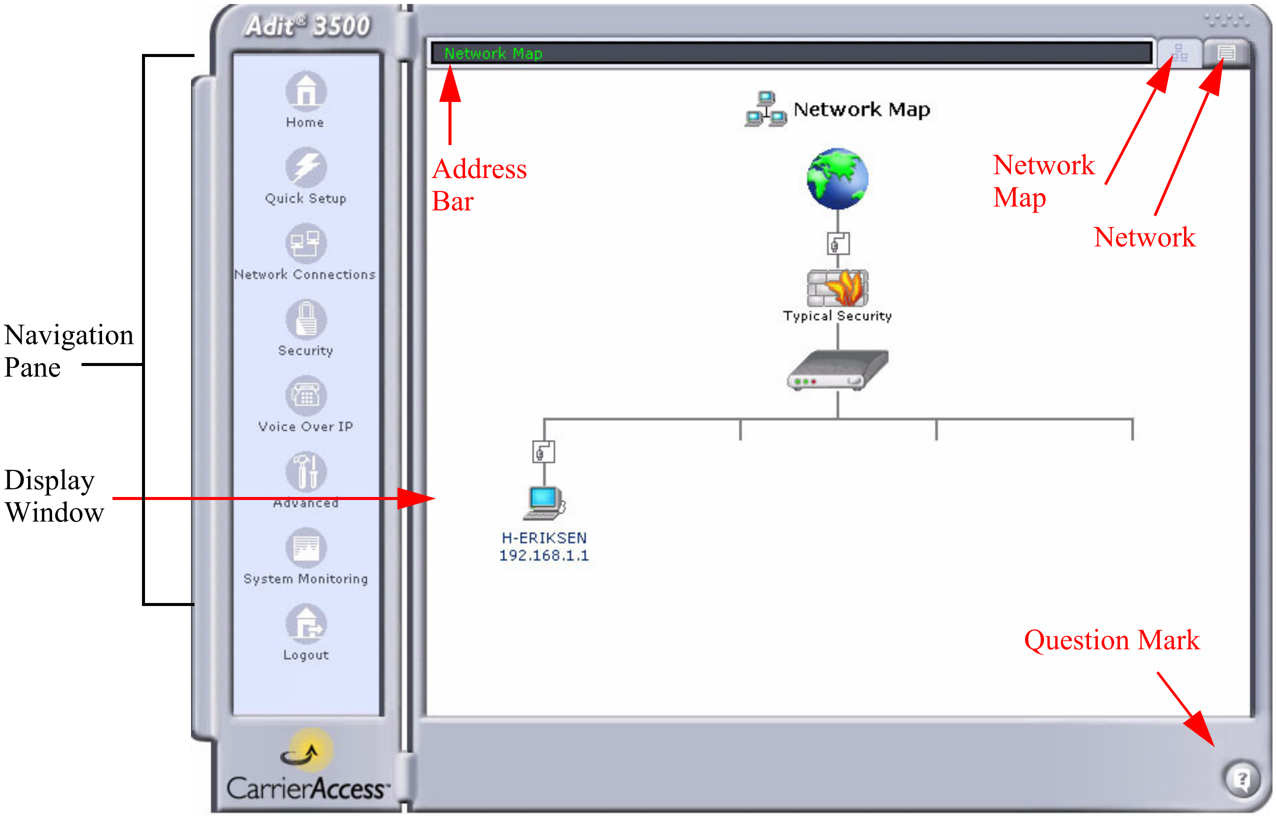
Overview

The GUI management window contains two sections:

- **Navigation Pane** (on the left) – Provides a list of topics to view and configure. When you select an icon, the information is displayed on the right.
- **Display window** (on the right) – Displays the setup windows for a topic selected from the Navigation Pane or items that have been selected through a shortcut button.

Other helpful features:

- **Address Bar** (along the top) – Displays the current path to the information displayed in the window below.
- **Network Map** (Button) – Provides a shortcut to the Network Map. See *Network Map* on page 1-7.
- **Network** (Button) – Displays the Network List.
- **Question Mark** (Button) – Provides a shortcut to Technical Information about the system.



Navigation Pane Icons

The following icons are available on the Navigation Pane:

Home - Displays the Network Map.

Quick Setup - Allows you to quickly configure your Internet connection.

Network Connections - Allows you to create and configure network connections.

Security - Allows you to configure the Firewall and regulate communication between the Internet and the network.

Voice Over IP - Allows you to configure VoIP features.
Note: This feature is not supported on the Adit 3200.

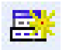
Advanced - Allows you to control network parameters (DHCP server, DNS) and perform administrative functions, including changing passwords and upgrading the system.

System Monitoring - Displays system information, statistics, logs, and alarms.

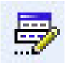
Logout - Logs you out of the current session.

Action Icons (for Managing Lists)

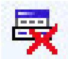
The following icons may appear in a list, under **Action**:



Add - Adds an item to the list.



Edit - Edits an item in the list.

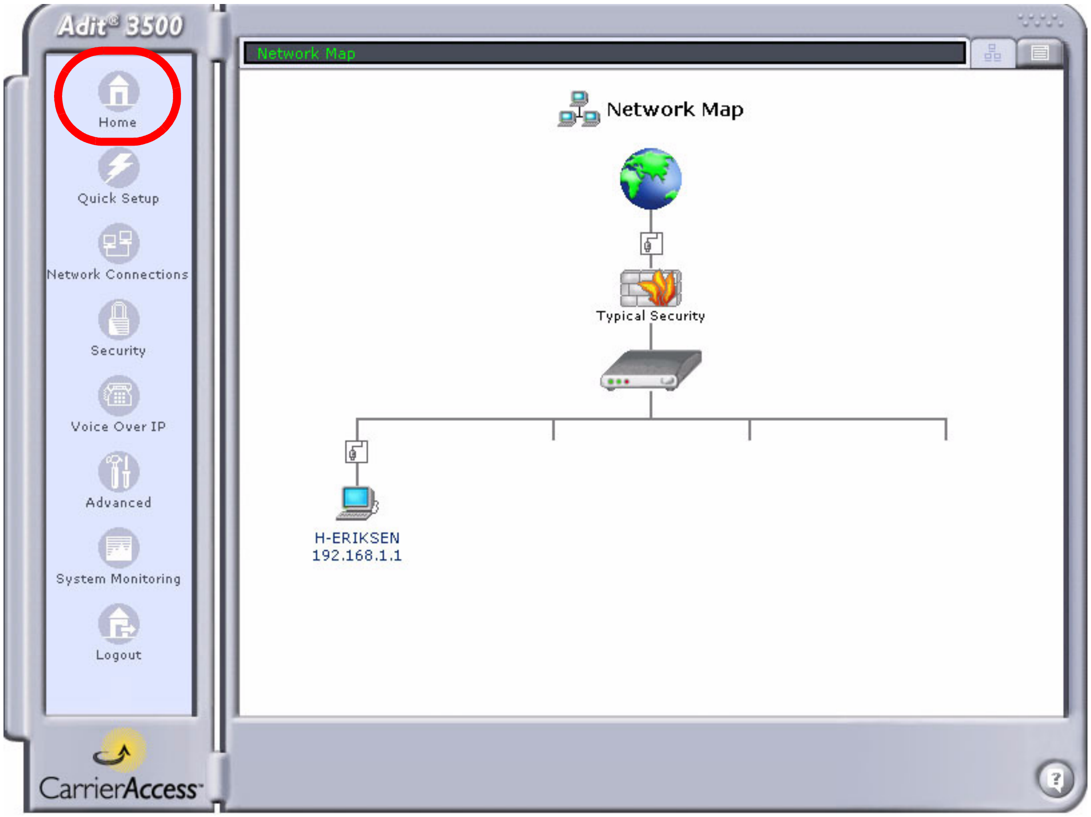


Delete - Removes an item from the list.

Home

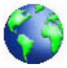
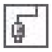
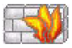
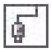
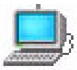
The Home window displays the Network Map which shows the various elements in the network.
Note: This window is modified as the configuration changes.

- Local network computers
- Firewall
- Adit 3000 or MSR
- External network interface (Internet connection)
- Internal network interface (Ethernet, etc.)



Network Map

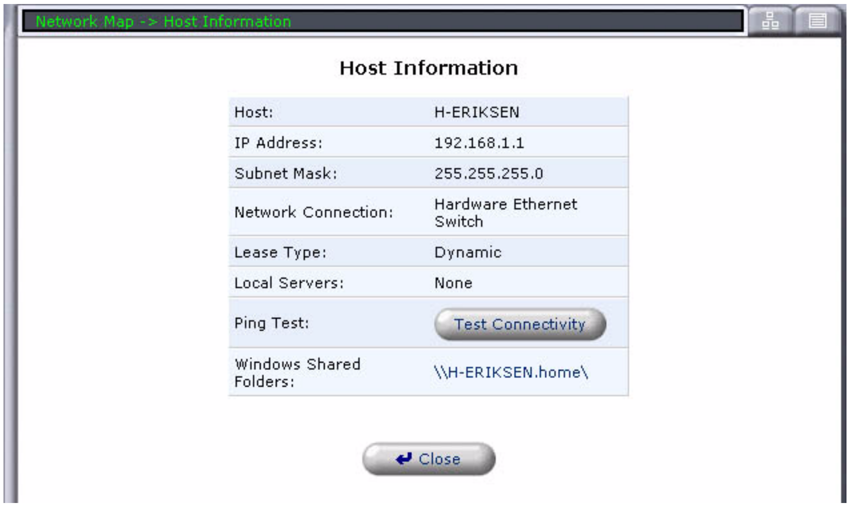
The following icons appear on the Network Map. For all icons except the Internet, you can open the item’s configuration window by clicking on the icon.

	Symbol	Represents
WAN		Internet. Opens the Quick Setup window.
		Ethernet WAN connection. Opens the Quick Setup window.
		Firewall. Opens the Security setup window. Note that the height of the wall corresponds to the security level currently selected.
LAN		Ethernet Local Area Network (LAN) connection. Opens the LAN Ethernet Properties window.
		A computer (host) connected in the network. Opens the Host Information window (see the following section). **Note:** This icon appears only when the host is connected with dynamic IP allocation. Hosts that have statically defined IPs are not shown.

Host Information Window

To display this window, click on the Computer Host icon on the Network Map.

The Host Information window displays network information for the corresponding computer.



Network Map -> Host Information

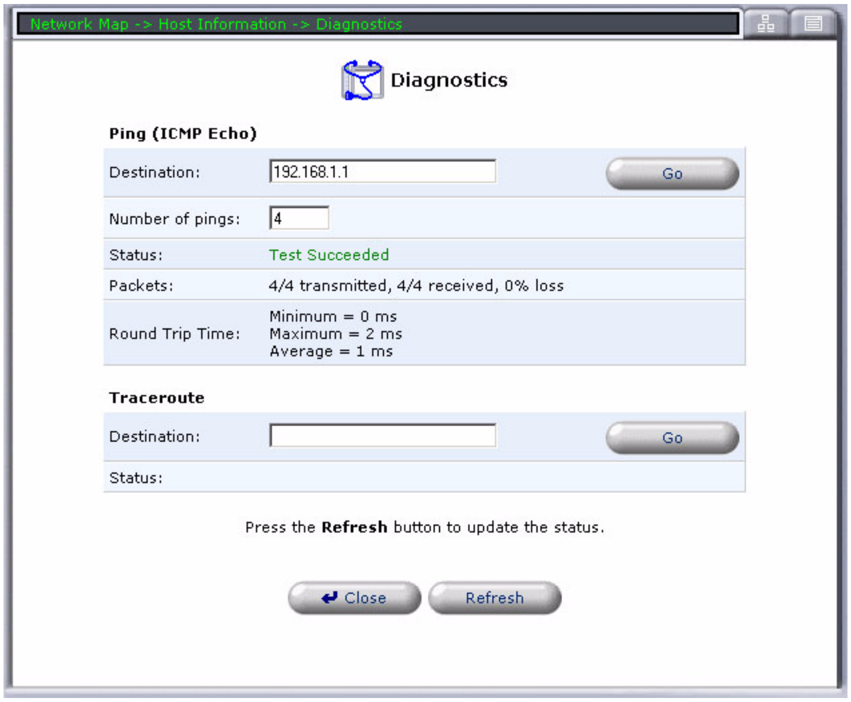
Host Information

Host:	H-ERIKSEN
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Network Connection:	Hardware Ethernet Switch
Lease Type:	Dynamic
Local Servers:	None
Ping Test:	Test Connectivity
Windows Shared Folders:	\\H-ERIKSEN.home\

Field	Definition
Host	Displays the Host Name.
IP Address	Displays the Host IP Address.
Subnet Mask	Displays the Subnet Mask of the Host IP Address.
Network Connection	Displays the type of Network Connection.
Lease Type	Displays the type of lease.
Local Servers	Displays the Local Server.
Ping Test	This button will test the connectivity through a Ping test. See the following section on **Test Connectivity**.
Windows Shared Folders	Displays an address for the host, which is also a link to the address.

Test Connectivity

The Test Connectivity button brings up the Diagnostics window. This window will automatically ping the Host IP Address and display the results.



Network Map -> Host Information -> Diagnostics

Diagnostics

Ping (ICMP Echo)

Destination:	192.168.1.1
Number of pings:	4
Status:	Test Succeeded
Packets:	4/4 transmitted, 4/4 received, 0% loss

Round Trip Time:	Minimum = 0 ms
	Maximum = 2 ms
	Average = 1 ms

Traceroute

Destination:	
Status:	

Press the **Refresh** button to update the status.

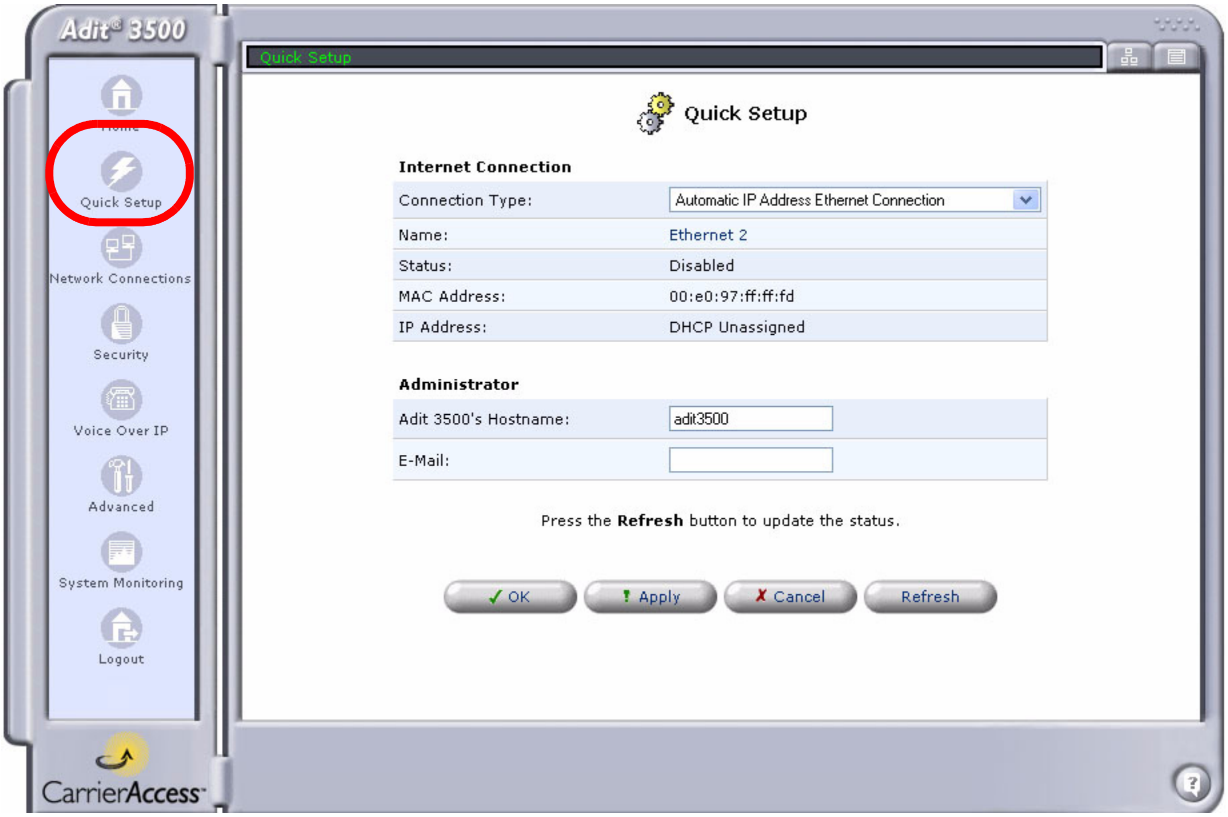
NOTE: This window can also be accessed through Advanced/Diagnostics. See *Diagnostics* on page 2-16, for detailed information on this window.

Quick Setup

The Quick Setup window enables quick configuration of your Internet connection.

When subscribing to a broadband service, you should be aware of the method by which you are connecting to the Internet. Technical information regarding the properties of your Internet connection should be provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you connect to the Internet using a static or dynamic IP address and what protocols, such as PPTP, you use to communicate over the Internet.

The Quick Setup window appears upon initial login, or it can opened by selecting the Quick Setup button on the navigation pane.



Quick Setup

Internet Connection

Connection Type:	Automatic IP Address Ethernet Connection
Name:	Ethernet 2
Status:	Disabled
MAC Address:	00:e0:97:ff:ff:fd
IP Address:	DHCP Unassigned

Administrator

Adit 3500's Hostname:	adit3500
E-Mail:	

Press the **Refresh** button to update the status.

Internet Connection

Connection Type

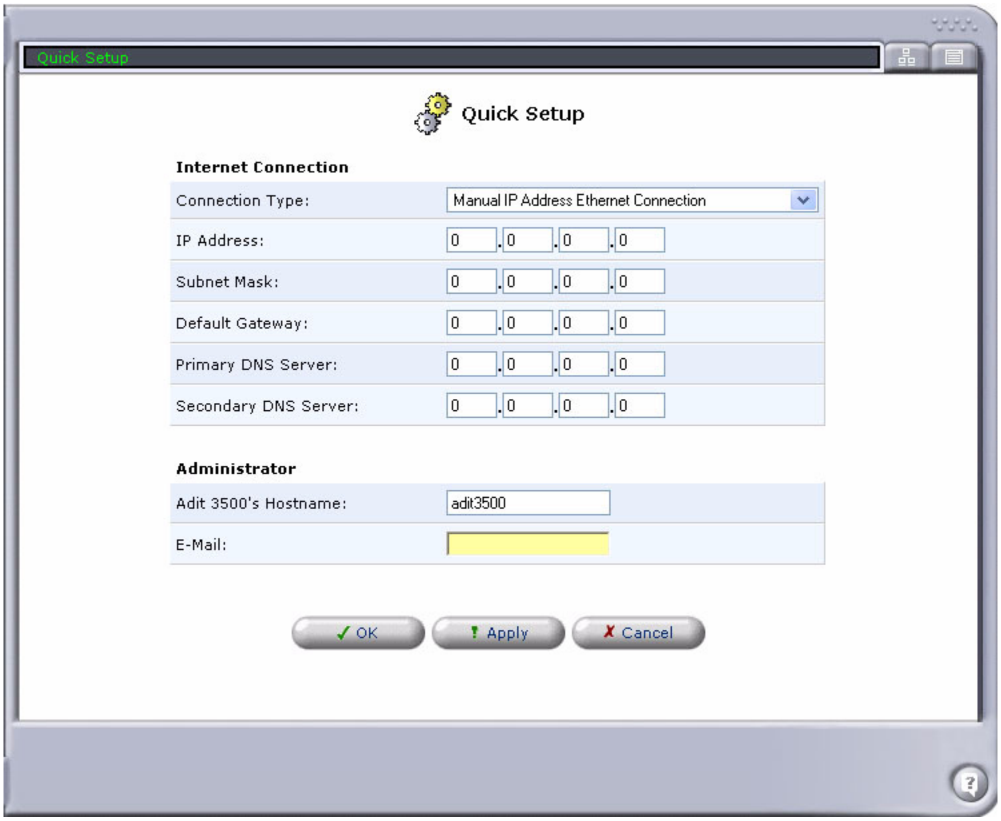
The WAN connection can be configured using any of the following methods. With each of these connection types, the window displays a different set of field options. See the following sections for information on each of these connection types and the associated options.

- **Manual IP Address Ethernet Connection**
- **Automatic IP Address Ethernet Connection**
- **Point-to-Point Protocol over DS0 (Serial)**
- **Multilink Point-to-Point Protocol over DS0 (Multilink)**
- **Point-to-Point Tunneling Protocol (PPTP)**
- **No Internet Connection**

Manual IP Address Ethernet Connection

This window is used to manually configure the Internet Connection with a specific IP Address.

Field	Definition
IP Address	Enter the IP Address for the Ethernet connection of this device.
Subnet Mask	Enter the Subnet Mask for the IP Address above.
Default Gateway	Enter the Default Gateway address for this device.
Primary DNS Server	Enter the Primary DNS Service address.
Secondary DNS Server	Enter the Secondary DNS Service address.



Internet Connection

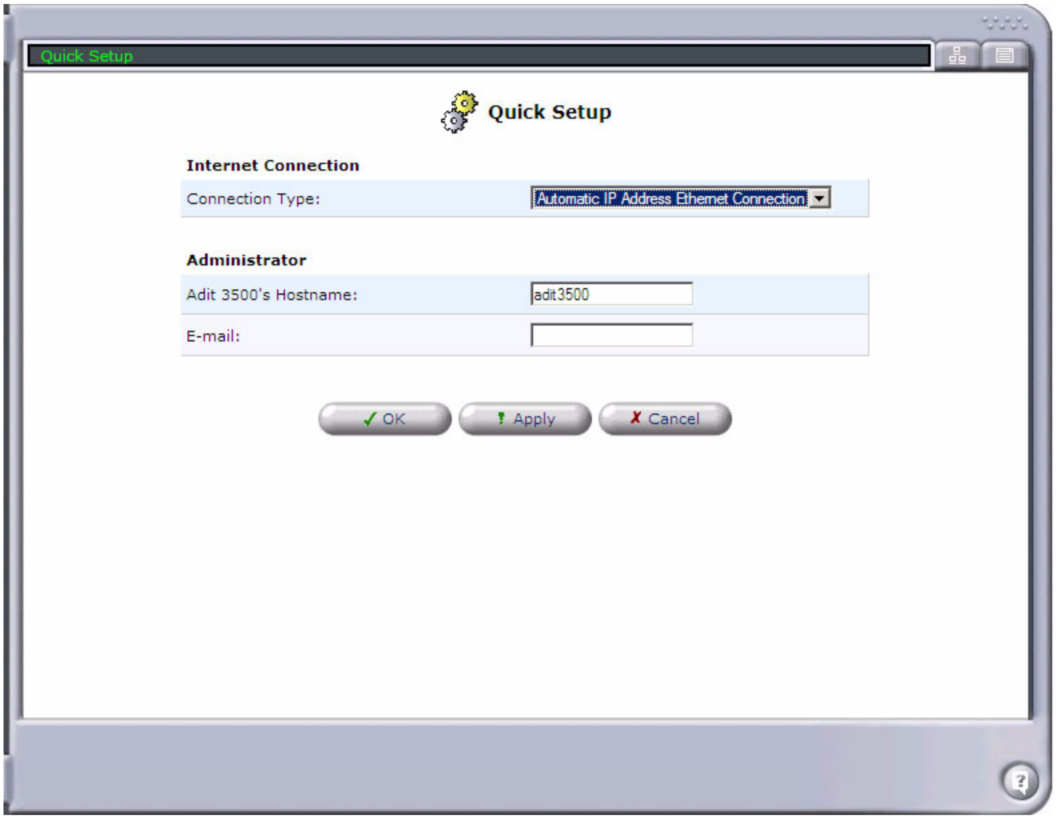
Connection Type:	Manual IP Address Ethernet Connection
IP Address:	0 .0 .0 .0
Subnet Mask:	0 .0 .0 .0
Default Gateway:	0 .0 .0 .0
Primary DNS Server:	0 .0 .0 .0
Secondary DNS Server:	0 .0 .0 .0

Administrator

Adit 3500's Hostname:	adit3500
E-Mail:	

Automatic IP Address Ethernet Connection

With this selection, the device uses DHCP to find and set an address for this connection.



Quick Setup

Internet Connection

Connection Type: Automatic IP Address Ethernet Connection

Administrator

Adit 3500's Hostname: adit3500

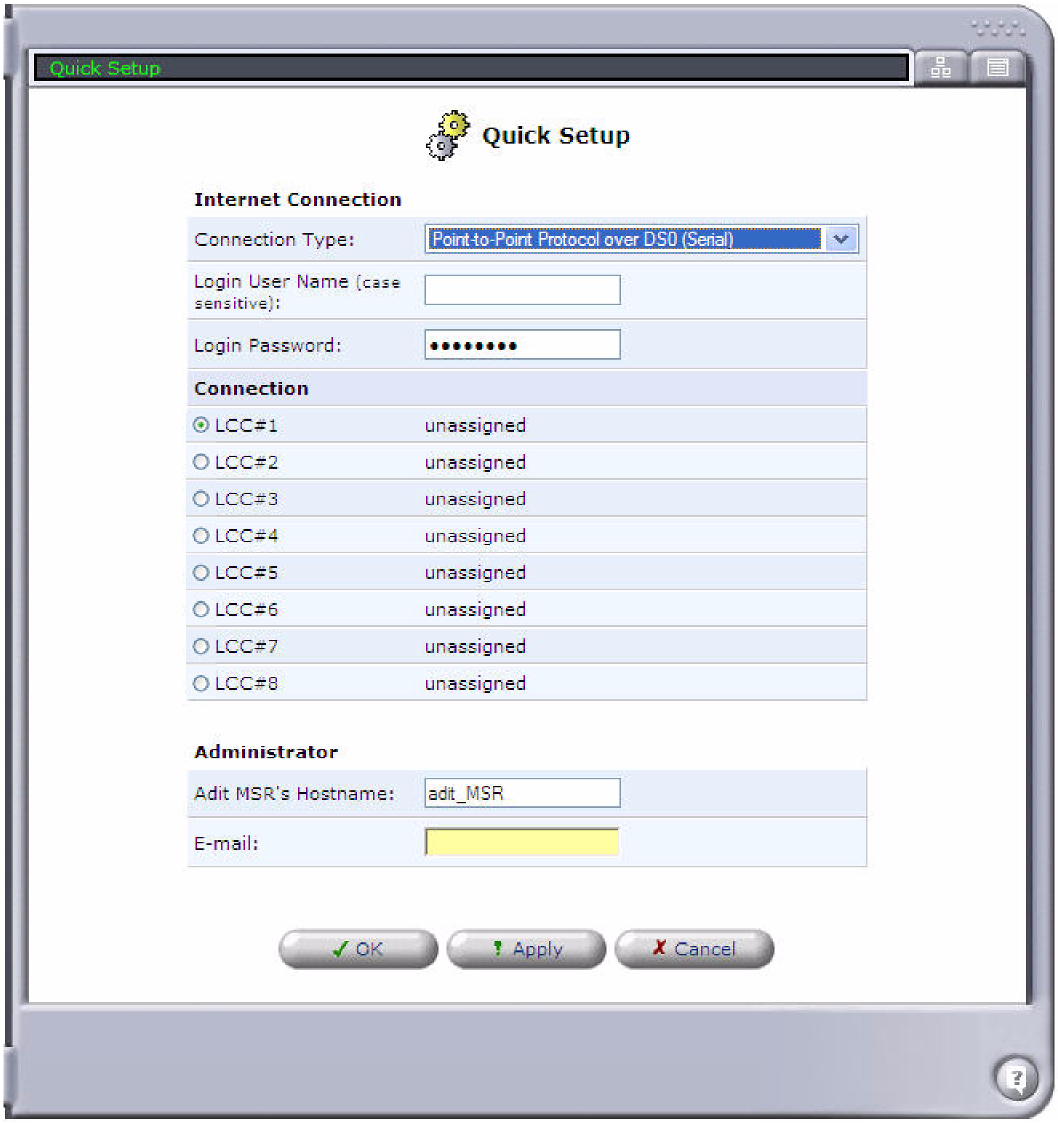
E-mail:

Point-to-Point Protocol over DS0 (Serial)

With this selection, the MSR card uses a single Link Cross-Connect (LCC) PPP WAN for Internet connectivity.

Field	Definition
Login User Name	Enter the user name for this unit.
Login Password	Enter the password for this unit.
Connection	Shows the LCCs available for the connection.

NOTE: For the MSR card, cross-connects from Adit 600 resources (T1 lines or WAN-capable cards) must be made before setting up the WAN link. All DS0s cross-connected to the WAN link must be of type "Data." Use the **connect (msr)** command to cross-connect resources to the MSR card. (See the *Adit 600 User Manual* for more information.)



Quick Setup

Internet Connection

Connection Type:	Point-to-Point Protocol over DS0 (Serial)
Login User Name (case sensitive):	
Login Password:	••••••••

Connection

● LCC#1	unassigned
○ LCC#2	unassigned
○ LCC#3	unassigned
○ LCC#4	unassigned
○ LCC#5	unassigned
○ LCC#6	unassigned
○ LCC#7	unassigned
○ LCC#8	unassigned

Administrator

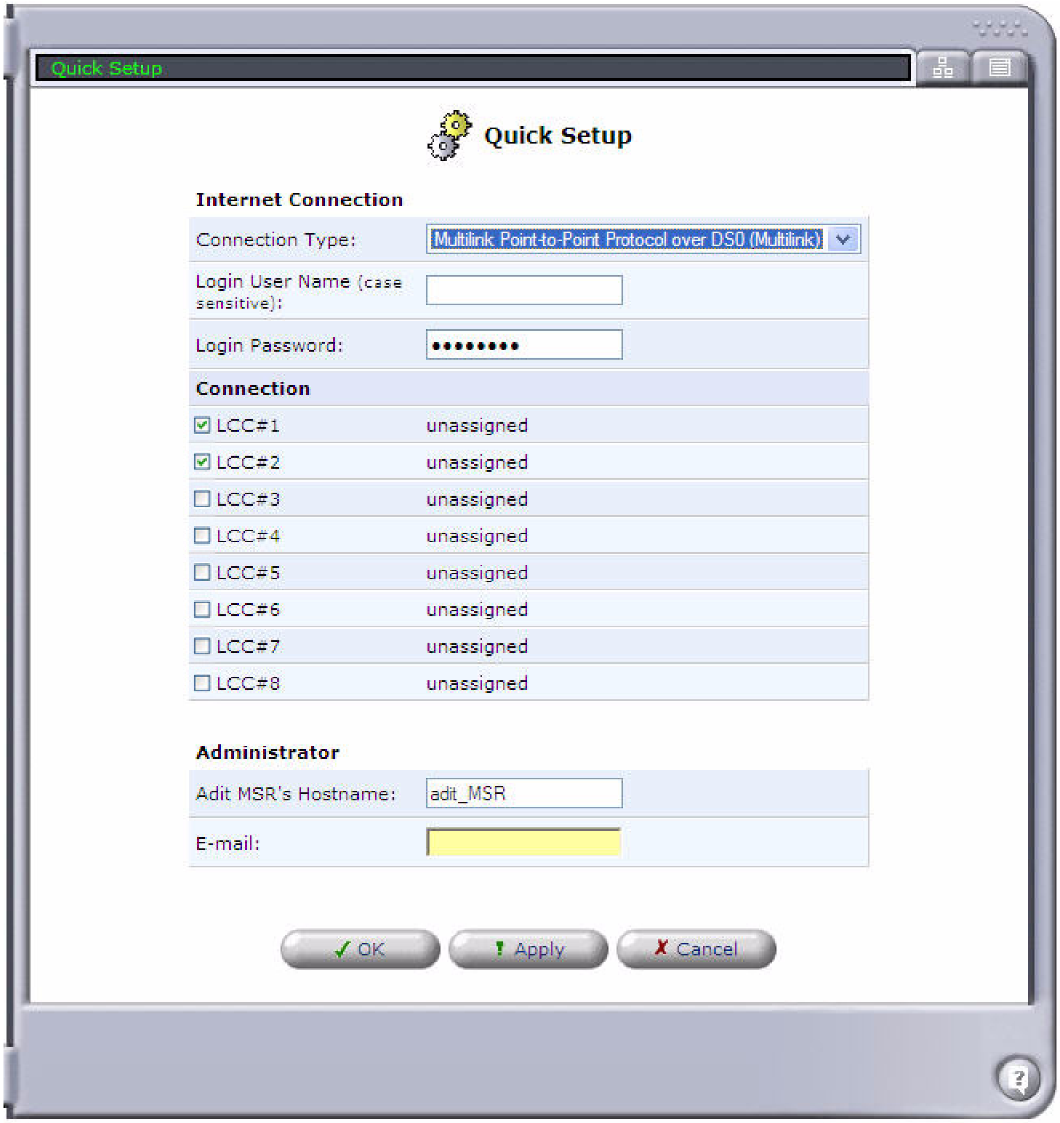
Adit MSR's Hostname:	adit_MSR
E-mail:	

Multilink Point-to-Point Protocol over DS0 (Multilink)

With this selection, the MSR card uses a multiple Link Cross-Connect (LCC) WAN for Internet connectivity.

Field	Definition
Login User Name	Enter the user name for this unit.
Login Password	Enter the password for this unit.
Connection	Shows the LCCs available for the connection.

NOTE: For the MSR card, cross-connects from Adit 600 resources (T1 lines or WAN-capable cards) must be made before setting up the WAN link. All DS0s cross-connected to the WAN link must be of type "Data." Use the **connect (msr)** command to cross-connect resources to the MSR card. (See the *Adit 600 User Manual* for more information.)



Quick Setup

Internet Connection

Connection Type:	Multilink Point-to-Point Protocol over DS0 (Multilink)
Login User Name (case sensitive):	
Login Password:	••••••••

Connection

☑ LCC#1	unassigned
☑ LCC#2	unassigned
□ LCC#3	unassigned
□ LCC#4	unassigned
□ LCC#5	unassigned
□ LCC#6	unassigned
□ LCC#7	unassigned
□ LCC#8	unassigned

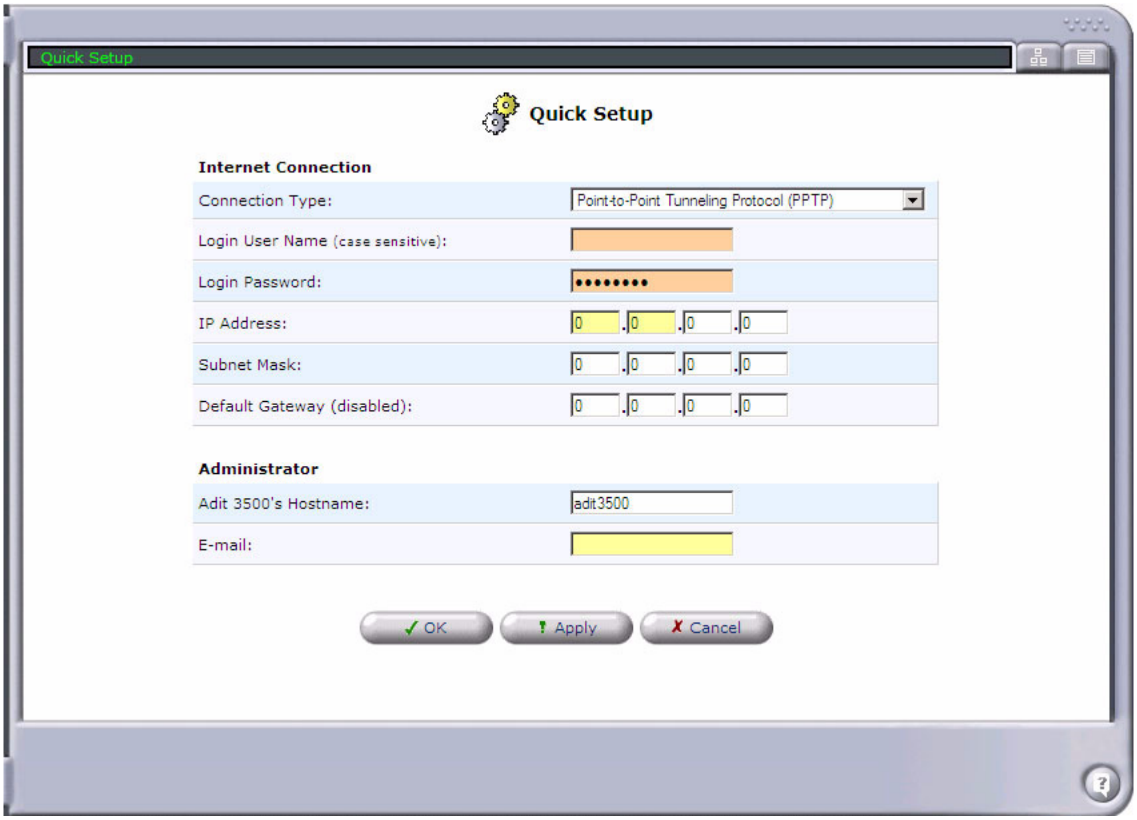
Administrator

Adit MSR's Hostname:	adit_MSR
E-mail:	

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling is a technology for creating Virtual Private Networks (VPNs). A VPN is a private network of computers that uses the public Internet to connect some nodes. Because the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is used to ensure that messages transmitted from one VPN node to another are secure. With PPTP, users can dial in to their corporate network via the Internet.

Field	Definition
Login User Name	Enter the User name for this unit.
Login Password	Enter the password for this unit.
IP Address	Enter the IP Address for the Ethernet connection of this device.
Subnet Mask	Enter the Subnet Mask for the IP Address above.
Default Gateway	Enter the Default Gateway address for this device.



Quick Setup

Internet Connection

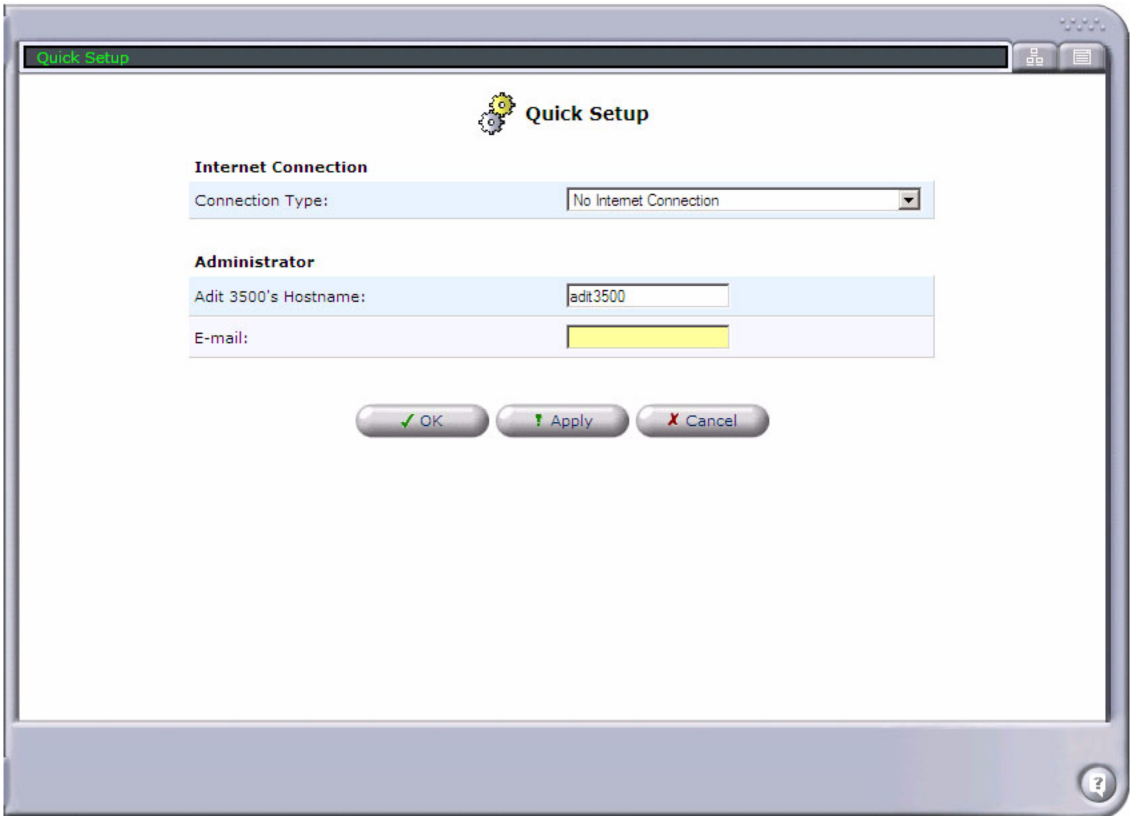
Connection Type:	Point-to-Point Tunneling Protocol (PPTP)
Login User Name (case sensitive):	
Login Password:	••••••••
IP Address:	0 .0 .0 .0
Subnet Mask:	0 .0 .0 .0
Default Gateway (disabled):	0 .0 .0 .0

Administrator

Adit 3500's Hostname:	adit3500
E-mail:	

No Internet Connection

This option disables the Internet connection on the device.



Internet Connection

Connection Type: No Internet Connection

Administrator

Adit 3500's Hostname: adit3500

E-mail:

Administrator

The following section appears on all Quick Setup windows (located at the bottom of the window)**.**

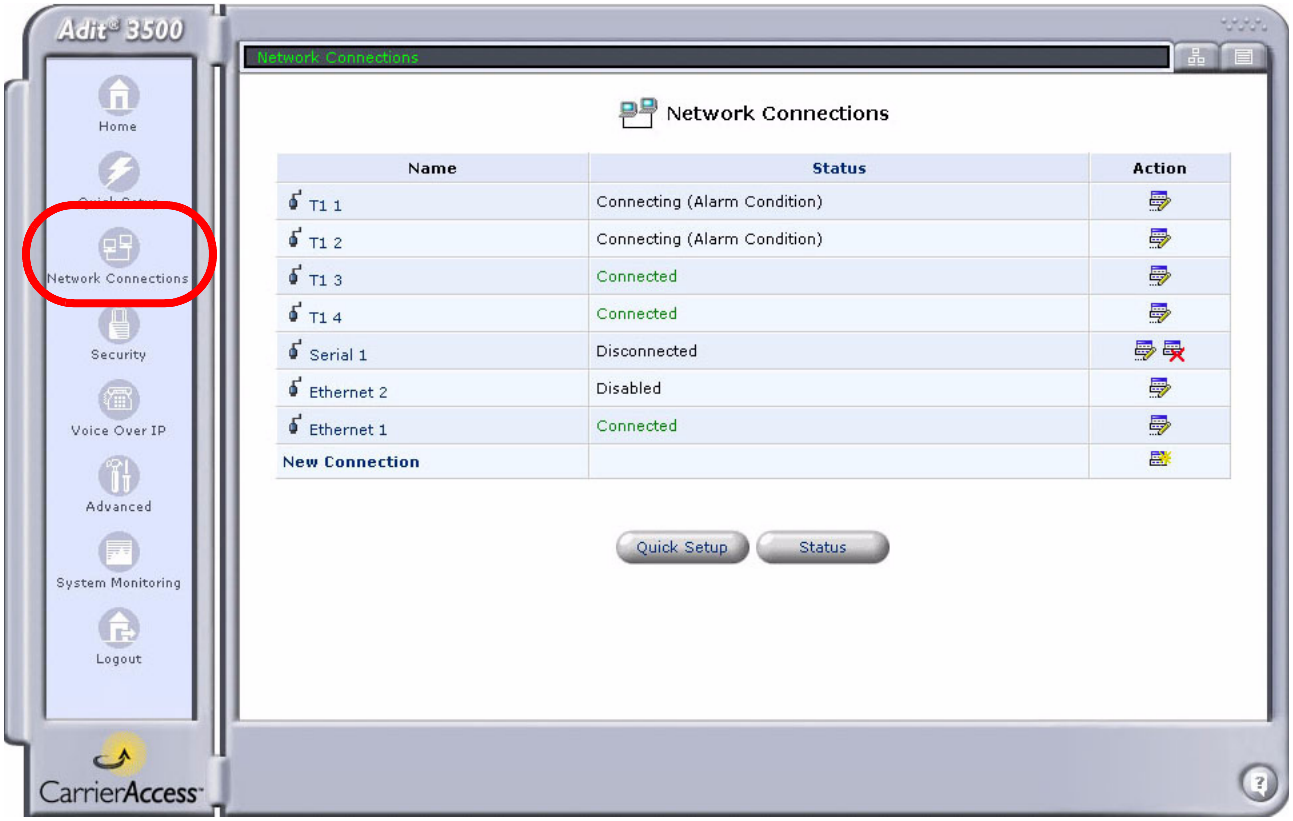
Field	Definition
Adit 3000's or Adit MSR's Hostname	Display/set the current the Host Name for this device.
E-Mail	Enter an E-Mail address to be used for monitoring and alert purposes.

Network Connections

The Network Connection window allows the user to create and configure network connections. For the Adit 3000, the basic connections for this system are preconfigured. Additional connections can be set up with the **New Connection** option.

For detailed information on Network Connections, see *Chapter 3, Network Connections*.

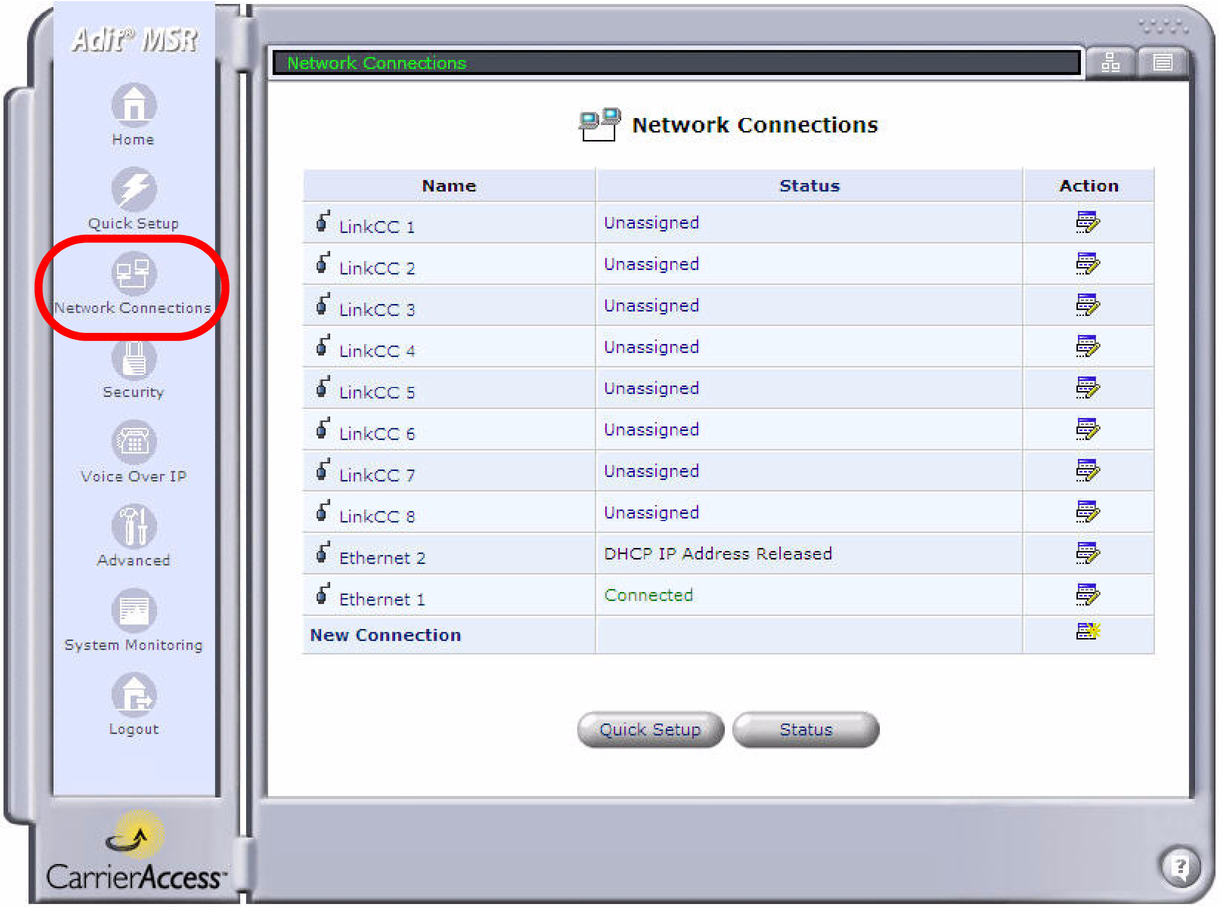
Adit 3500



Network Connections

Name	Status	Action
T1 1	Connecting (Alarm Condition)	✎
T1 2	Connecting (Alarm Condition)	✎
T1 3	Connected	✎
T1 4	Connected	✎
Serial 1	Disconnected	✎ ✗
Ethernet 2	Disabled	✎
Ethernet 1	Connected	✎
New Connection		✱

Adit MSR



Network Connections

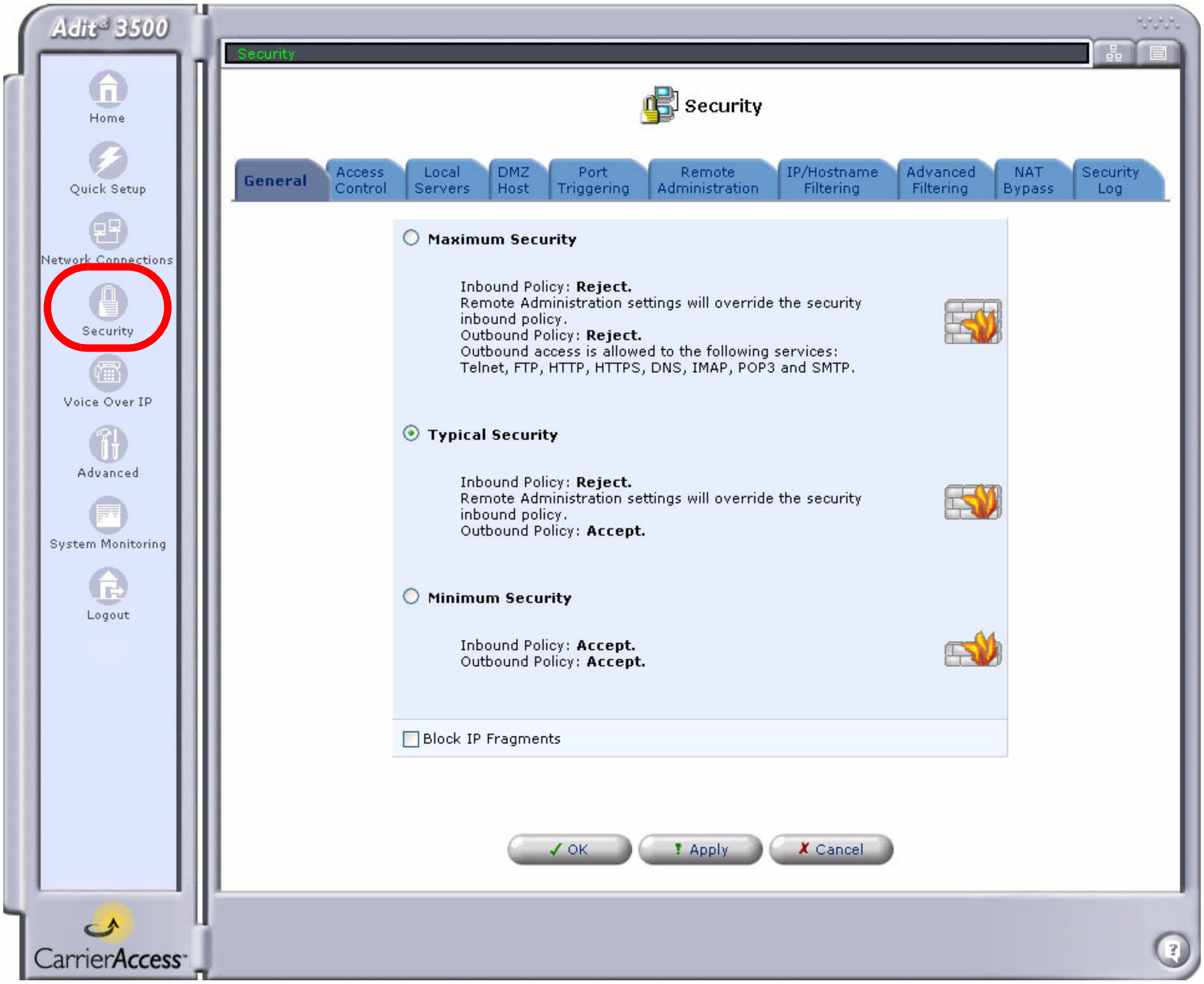
Name	Status	Action
LinkCC 1	Unassigned	
LinkCC 2	Unassigned	
LinkCC 3	Unassigned	
LinkCC 4	Unassigned	
LinkCC 5	Unassigned	
LinkCC 6	Unassigned	
LinkCC 7	Unassigned	
LinkCC 8	Unassigned	
Ethernet 2	DHCP IP Address Released	
Ethernet 1	Connected	
New Connection		

Security

The Adit 3000 and MSR include comprehensive and robust security services:

- Stateful Packet Inspection Firewall
- User authentication protocols
- Password protection mechanisms

For detailed information on security features, see *Chapter 4, Security*.



○ **Maximum Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services:
Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ **Minimum Security**

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

□ Block IP Fragments

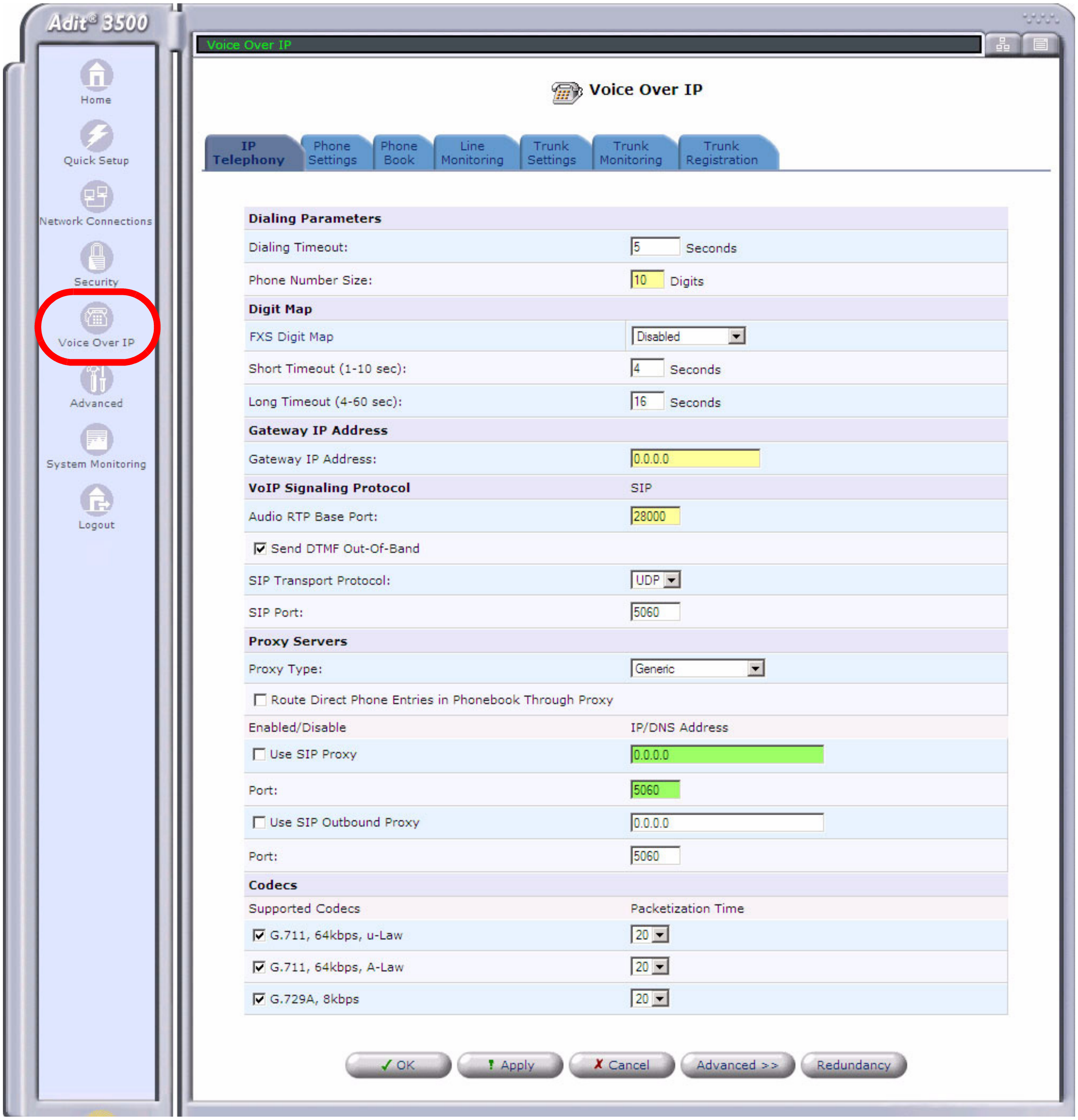
Voice over IP

The VoIP feature allows you to connect multiple phones over a single broadband connection, providing the benefits and quality of digital voice. The Adit 3104, 3500, and MSR enable you to place and receive calls over the Internet using a standard telephone set connected to the Adit.

For detailed information on VoIP features, see *Chapter 6, Voice Over IP*.

NOTE: This feature is not supported by the Adit 3200.

WARNING! **ANY CHANGES TO THE VOIP SETTINGS WILL RESTART THE VOIP TASK AND WILL CAUSE ANY ACTIVE CALLS TO BE DROPPED.**



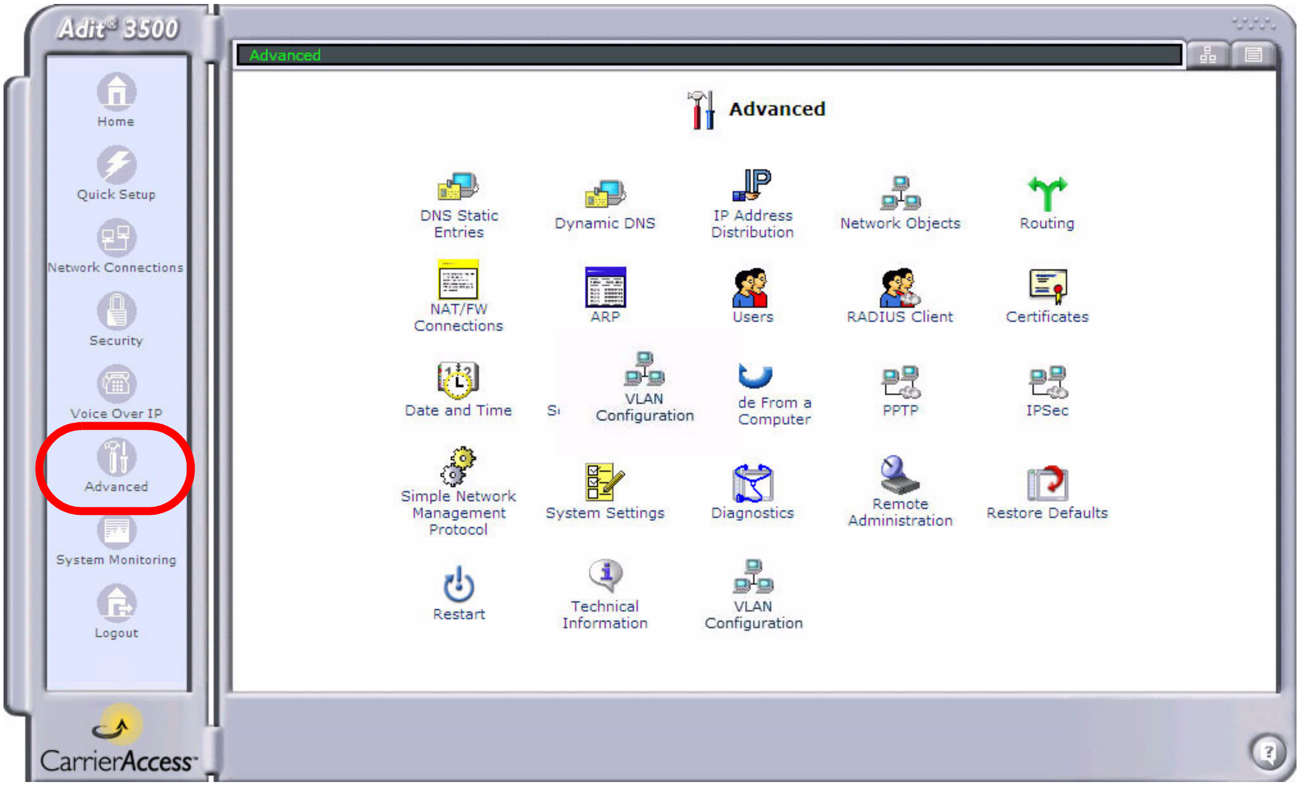
Voice Over IP

Dialing Parameters	
Dialing Timeout:	5 Seconds
Phone Number Size:	10 Digits
Digit Map	
FXS Digit Map	Disabled
Short Timeout (1-10 sec):	4 Seconds
Long Timeout (4-60 sec):	16 Seconds
Gateway IP Address	
Gateway IP Address:	0.0.0.0
VoIP Signaling Protocol	SIP
Audio RTP Base Port:	28000
☑ Send DTMF Out-Of-Band	
SIP Transport Protocol:	UDP
SIP Port:	5060
Proxy Servers	
Proxy Type:	Generic
☐ Route Direct Phone Entries in Phonebook Through Proxy	
Enabled/Disable	IP/DNS Address
☐ Use SIP Proxy	0.0.0.0
Port:	5060
☐ Use SIP Outbound Proxy	0.0.0.0
Port:	5060
Codecs	
Supported Codecs	Packetization Time
☑ G.711, 64kbps, u-Law	20
☑ G.711, 64kbps, A-Law	20
☑ G.729A, 8kbps	20

Advanced

This section of the Management Console is intended primarily for more advanced users. Some changes to settings within this section could adversely affect the operation of the Adit and the network, and should be made with caution.

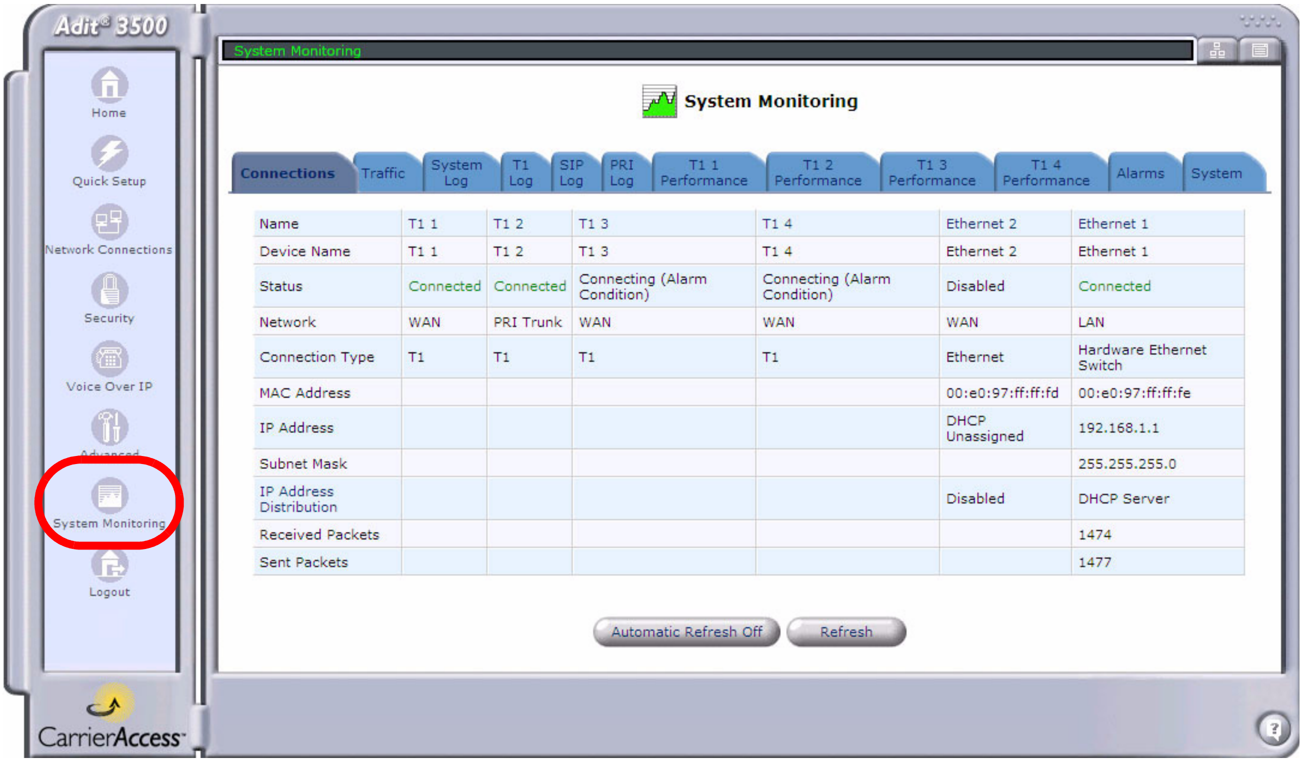
For detailed information on Advanced features, see *Chapter 2, Advanced*.



System Monitoring

The System Monitoring window displays important system information that can be used to monitor and troubleshoot the system. Connection status, alarms, system information, and logs are all accessible through this window.

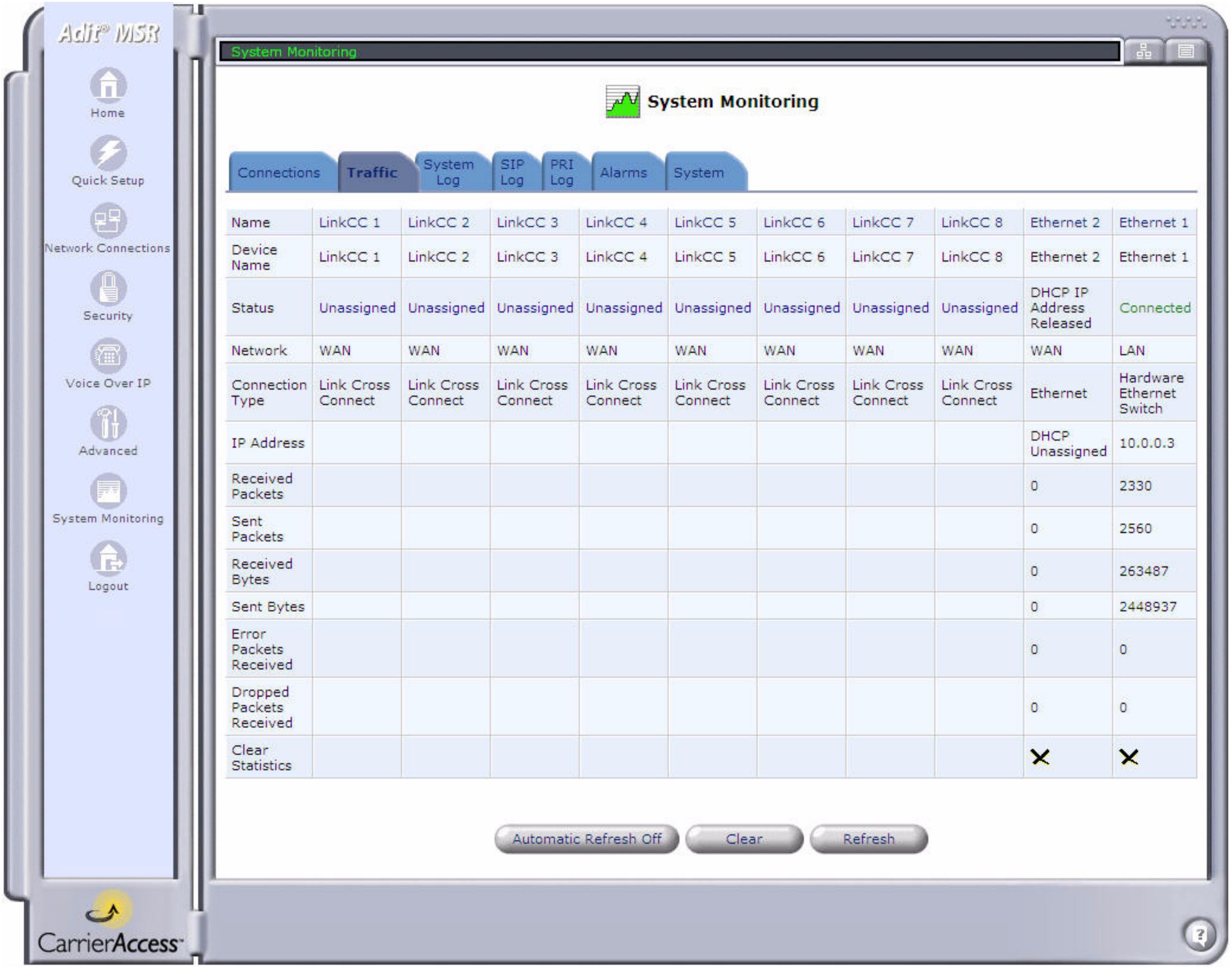
Adit 3500



System Monitoring

Name	T1 1	T1 2	T1 3	T1 4	Ethernet 2	Ethernet 1
Device Name	T1 1	T1 2	T1 3	T1 4	Ethernet 2	Ethernet 1
Status	Connected	Connected	Connecting (Alarm Condition)	Connecting (Alarm Condition)	Disabled	Connected
Network	WAN	PRI Trunk	WAN	WAN	WAN	LAN
Connection Type	T1	T1	T1	T1	Ethernet	Hardware Ethernet Switch
MAC Address					00:e0:97:ff:ff:fd	00:e0:97:ff:ff:fe
IP Address					DHCP Unassigned	192.168.1.1
Subnet Mask						255.255.255.0
IP Address Distribution					Disabled	DHCP Server
Received Packets						1474
Sent Packets						1477

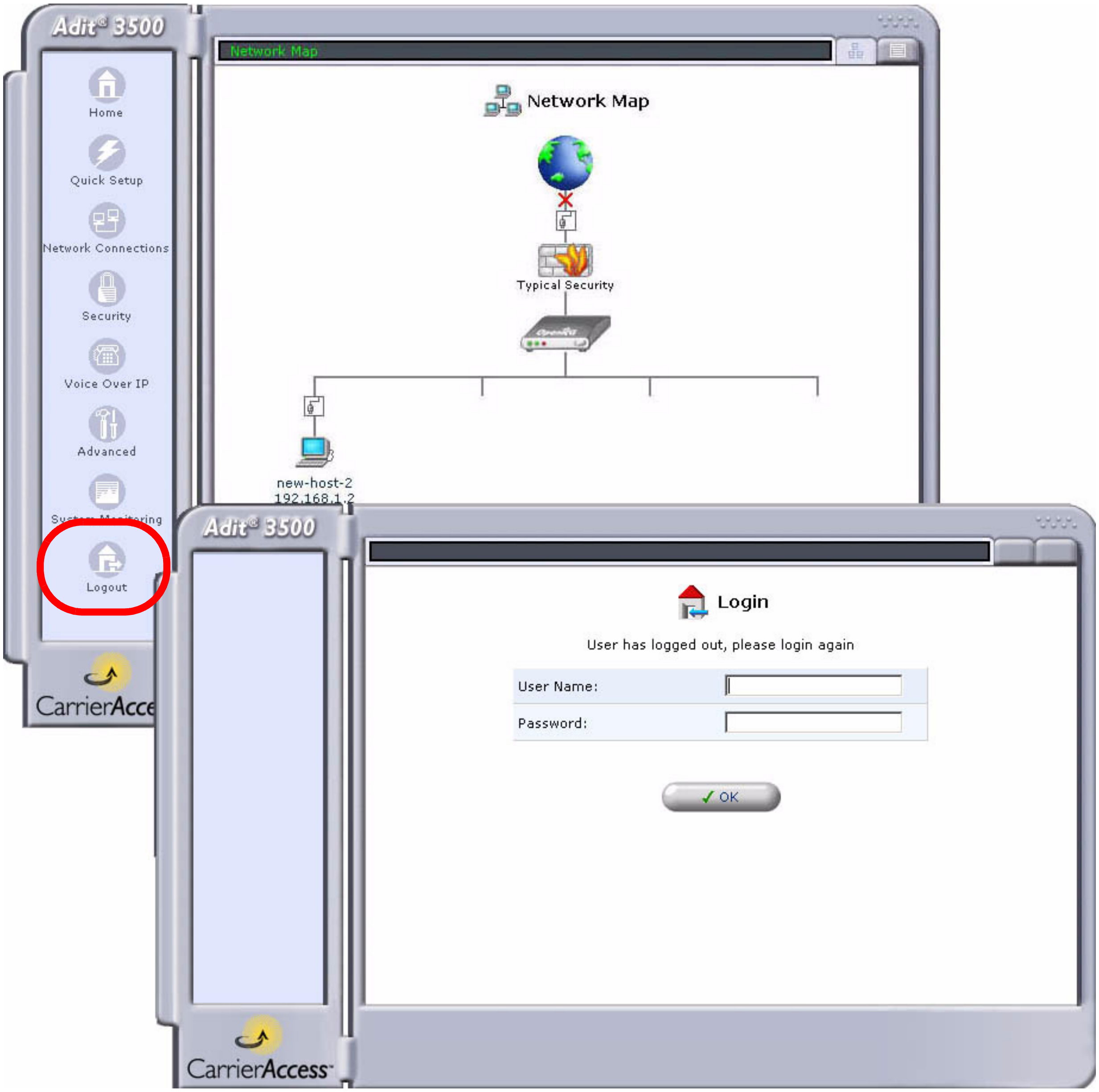
Adit MSR



Name	LinkCC 1	LinkCC 2	LinkCC 3	LinkCC 4	LinkCC 5	LinkCC 6	LinkCC 7	LinkCC 8	Ethernet 2	Ethernet 1
Device Name	LinkCC 1	LinkCC 2	LinkCC 3	LinkCC 4	LinkCC 5	LinkCC 6	LinkCC 7	LinkCC 8	Ethernet 2	Ethernet 1
Status	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	DHCP IP Address Released	Connected
Network	WAN	WAN	WAN	WAN	WAN	WAN	WAN	WAN	WAN	LAN
Connection Type	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Ethernet	Hardware Ethernet Switch
IP Address									DHCP Unassigned	10.0.0.3
Received Packets									0	2330
Sent Packets									0	2560
Received Bytes									0	263487
Sent Bytes									0	2448937
Error Packets Received									0	0
Dropped Packets Received									0	0
Clear Statistics									✕	✕

Logout

The Logout feature logs the user out of the system and returns to the Login window.



User has logged out, please login again

User Name:
Password:

CHAPTER 2

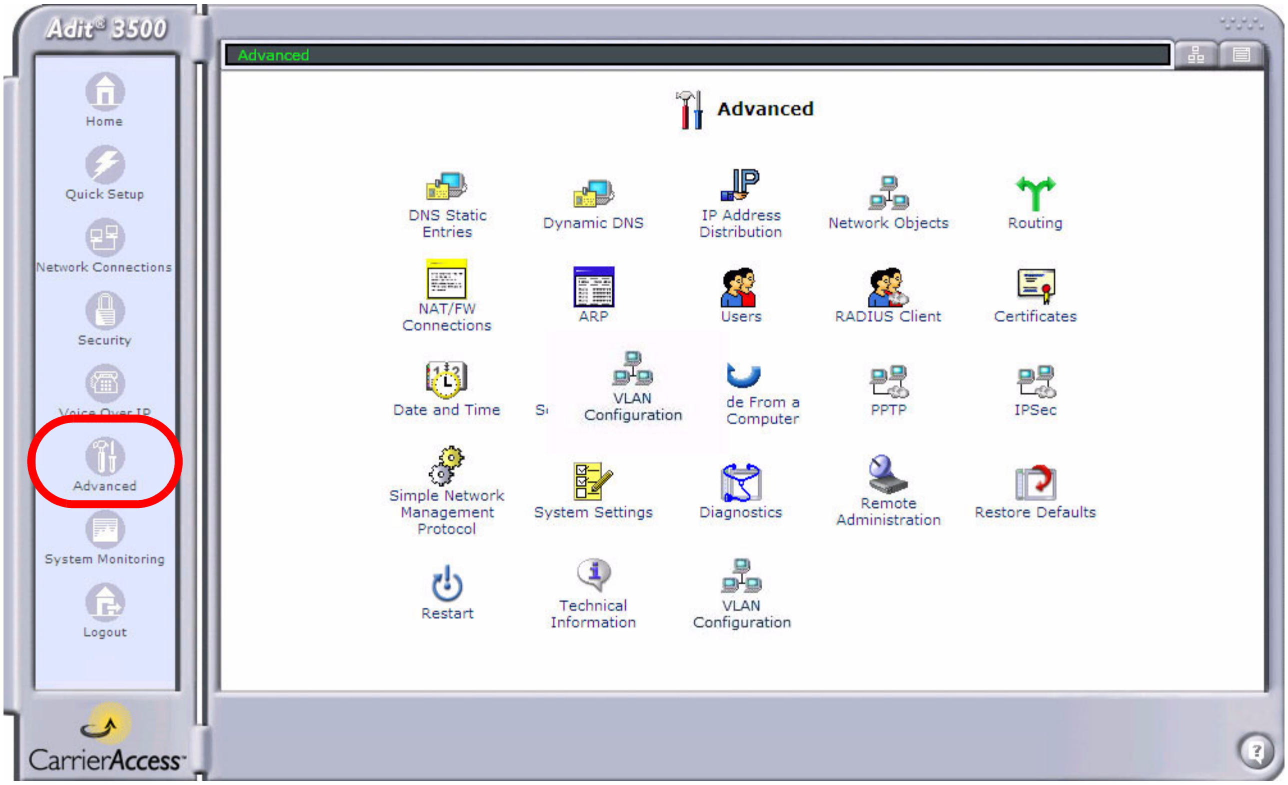
Advanced

In this Chapter

- Overview
- ARP
- Certificates
- Date and Time
- Diagnostics
- DNS Static Entries
- Dynamic DNS
- IP Address Distribution (DHCP)
- IPSec (IP Security)
- NAT/FW Connections
- Network Objects
- PPTP (Point-to-Point Tunneling Protocol)
- RADIUS Client
- Remote Administration
- Restart
- Restore Defaults
- Routing
- Scheduler Rules
- Simple Network Management Protocol
- System Settings
- Technical Information
- Upgrade From a Local Computer
- Users
- VLAN Configuration

Overview

This section of the Management Console is intended primarily for more advanced users. Some changes to settings within this section could adversely affect the operation of the system and the network, and should be made with caution.

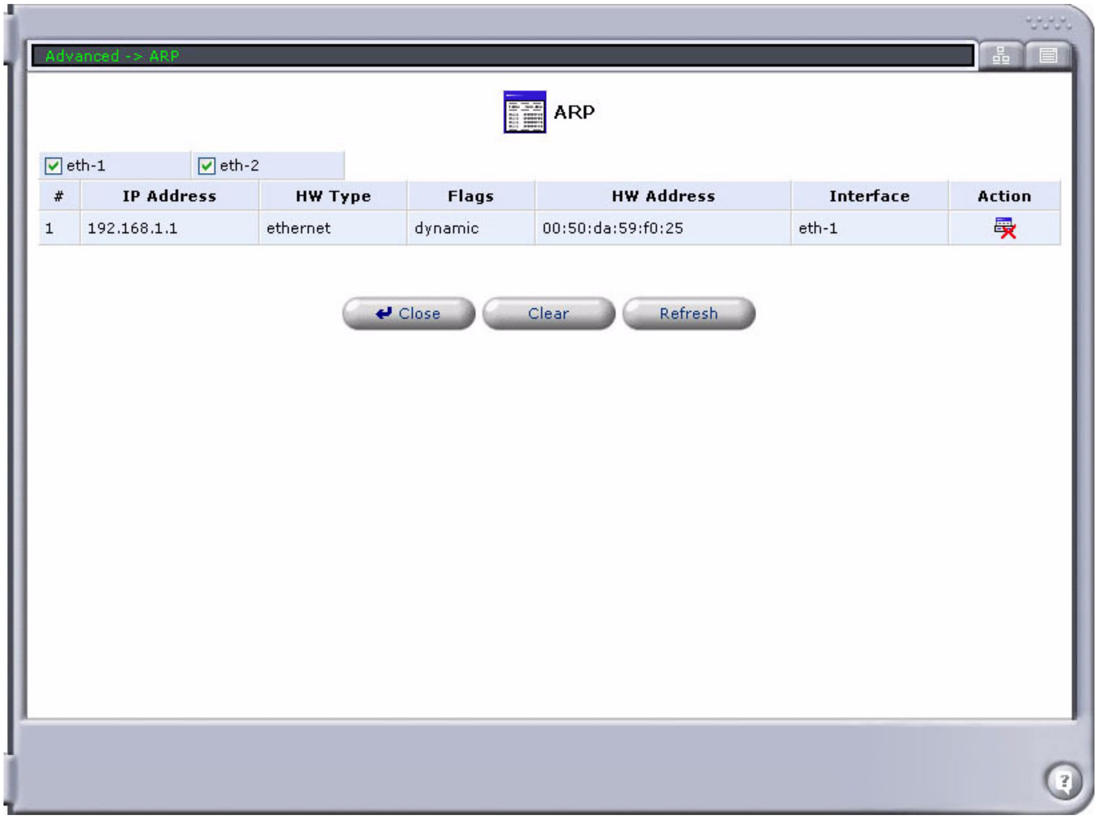


ARP

The ARP (Address Resolution Protocol) window displays the current ARP table.

There are display options:

- **eth-1** - When checked, displays the LAN Ethernet ARP.
- **eth-2** - When checked, displays the WAN Ethernet ARP.
- **Clear** - Clears those entries related with the interface(s) from the display.
- **Refresh** - Refreshes the ARP table.



☑ eth-1 ☑ eth-2

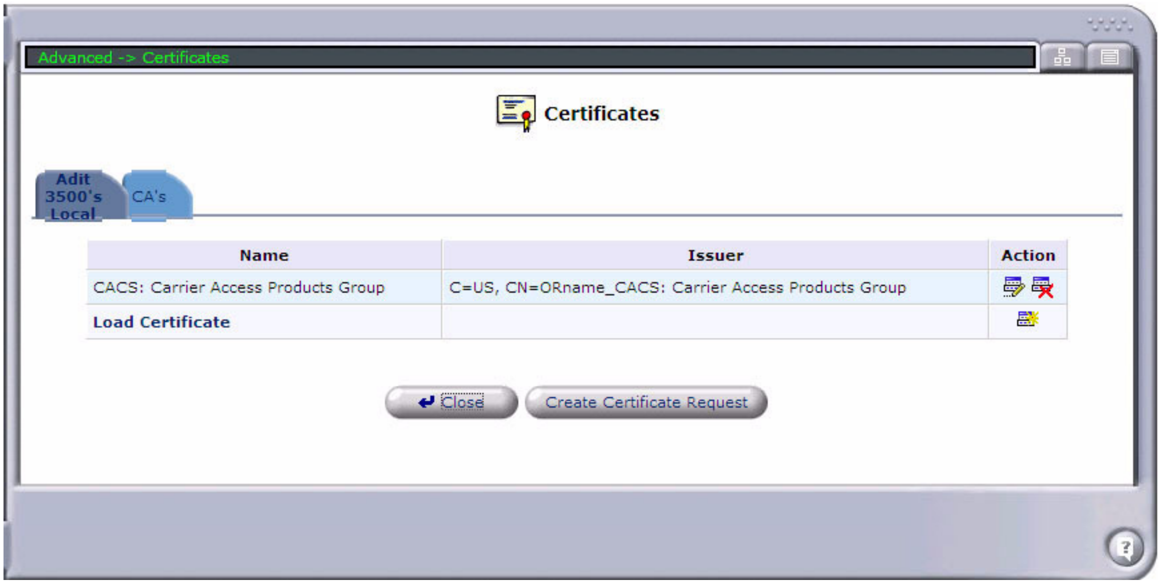
#	IP Address	HW Type	Flags	HW Address	Interface	Action
1	192.168.1.1	ethernet	dynamic	00:50:da:59:f0:25	eth-1	✗

Certificates

Public-key cryptography uses a pair of keys:

- Public Key, which encrypts data (known to the world)
- A corresponding private key for decryption (secret)

Anyone with access to your public key can encrypt information, but only the person who has the corresponding private key can decrypt the information.



Name	Issuer	Action
CACS: Carrier Access Products Group	C=US, CN=ORname_CACS: Carrier Access Products Group	
Load Certificate		

Digital Certificates

When working with public-key cryptography, the user must be careful and verify that the correct public key is used. Man-in-the-middle attacks pose a potential threat, where an ill-intending 3rd party posts a phony key with the name and user ID on an intended recipient. Data transfer that is intercepted by the owner of the counterfeit key can fall in the wrong hands.

Digital certificates provide a means for establishing whether a public key truly belongs to the supposed owner. It is a digital form of credentials. It has information on it that identifies you, and an authorized statement to the effect that someone else has confirmed your identity.

Digital certificates are used to foil attempts by an ill-intending party to use an unauthorized public key. A digital certificate consists of the following:

- A Public Key
- Certificate Information - the “identity” of the user (name, user ID, etc.).
- Digital Signatures - A statement stating that the information enclosed in the certificate has been vouched for by a Certificate Authority (CA).

Binding this information together, a certificate is a public key with identification forms attached, coupled with a stamp of approval by a trusted party.

X.509 Certificate Format

The Adit 3000 and Adit MSR support X.509 certificates that comply with the ITU-T X.509 international standard. An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it (the data format). All X.509 certificates have the following data:

- **Certificate holder's public key** - the public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters.
- **Serial number of the certificate** - the entity that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it issues.
- **Certificate holder's unique identifier** - this name is intended to be unique across the Internet and consists of multiple subsections.
- **Certificate's validity period** - the certificate's start date/time and expiration date/time, indicates when the certificate will expire.
- **Unique name of the certificate issuer** - the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate.
- **Digital signature of the issuer** - the signature using the private key of the entity that issued the certificate.
- **Signature algorithm identifier** - identifies the algorithm used by the CA to sign the certificate.

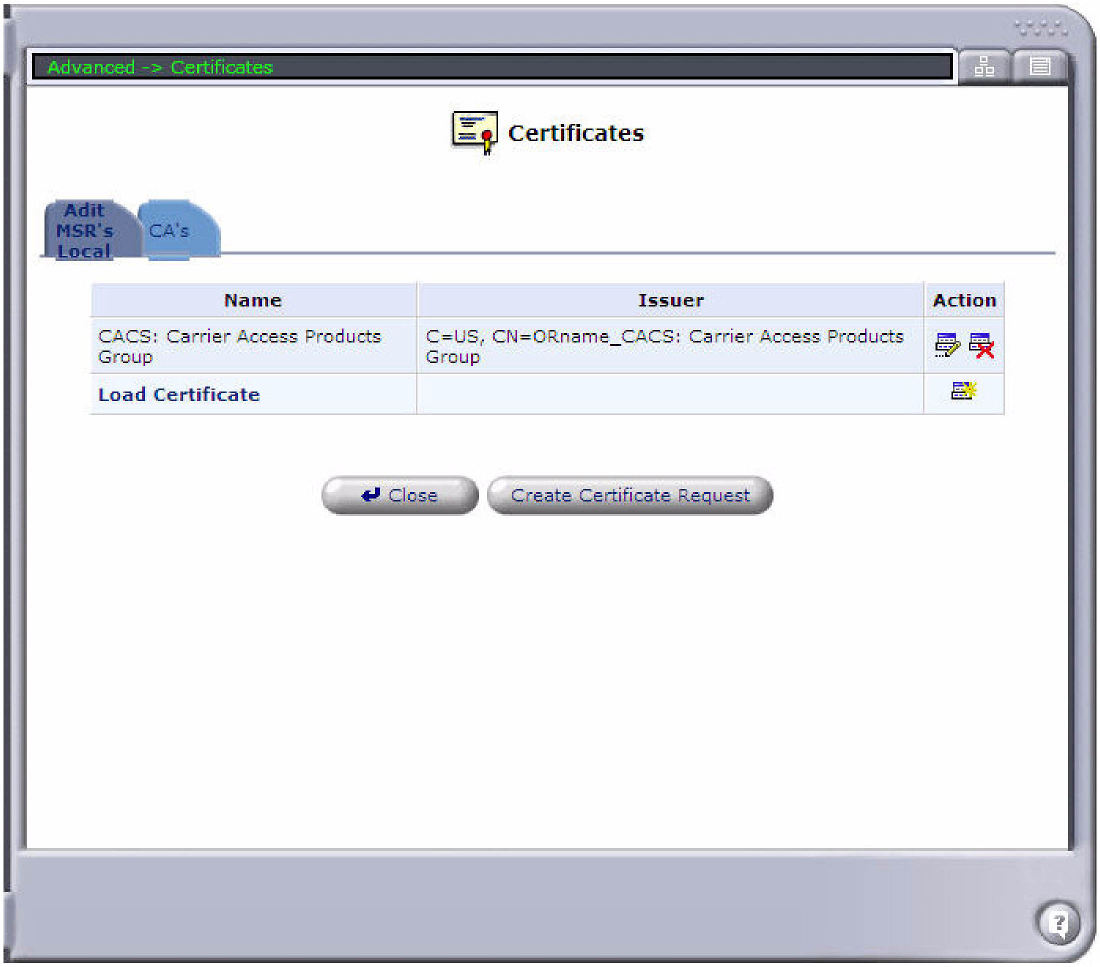
Obtaining and Loading an X.509 Certificate

To obtain an X509 certificate, you must ask a CA to issue you one. You provide your public key, proof that you possess the corresponding private key, and some specific information about yourself. You then digitally sign the information and send the whole package (the certificate request) to the CA. The CA then performs some due diligence in verifying that the information you provided is correct and, if so, generates the certificate and returns it.

You might think of an X509 certificate as looking like a standard paper certificate with a public key taped to it. It has your name and some information about you on it, plus the signature of the person who issued it to you.

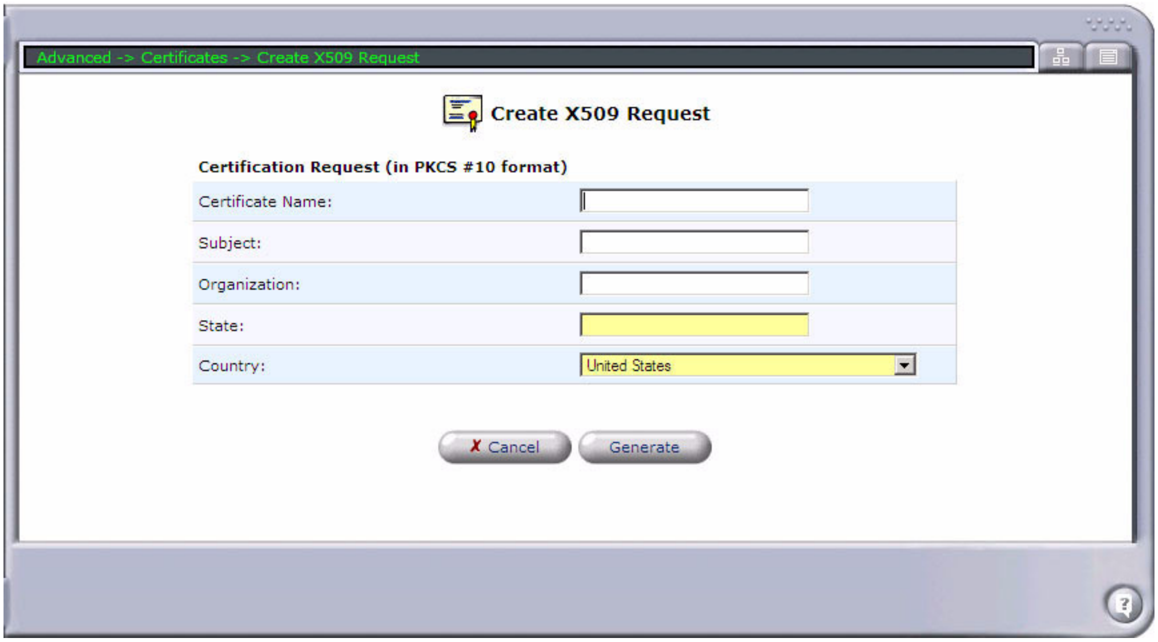
To obtain and load an X.509 certificate:

1. Select **Advanced/ Certificates**.



Name	Issuer	Action
CACS: Carrier Access Products Group	C=US, CN=ORname_CACS: Carrier Access Products Group	
Load Certificate		

2. On the **Adit 3000 or Adit MSR's Local** tab, select the **Create Certificate Request** button.



Advanced -> Certificates -> Create X509 Request

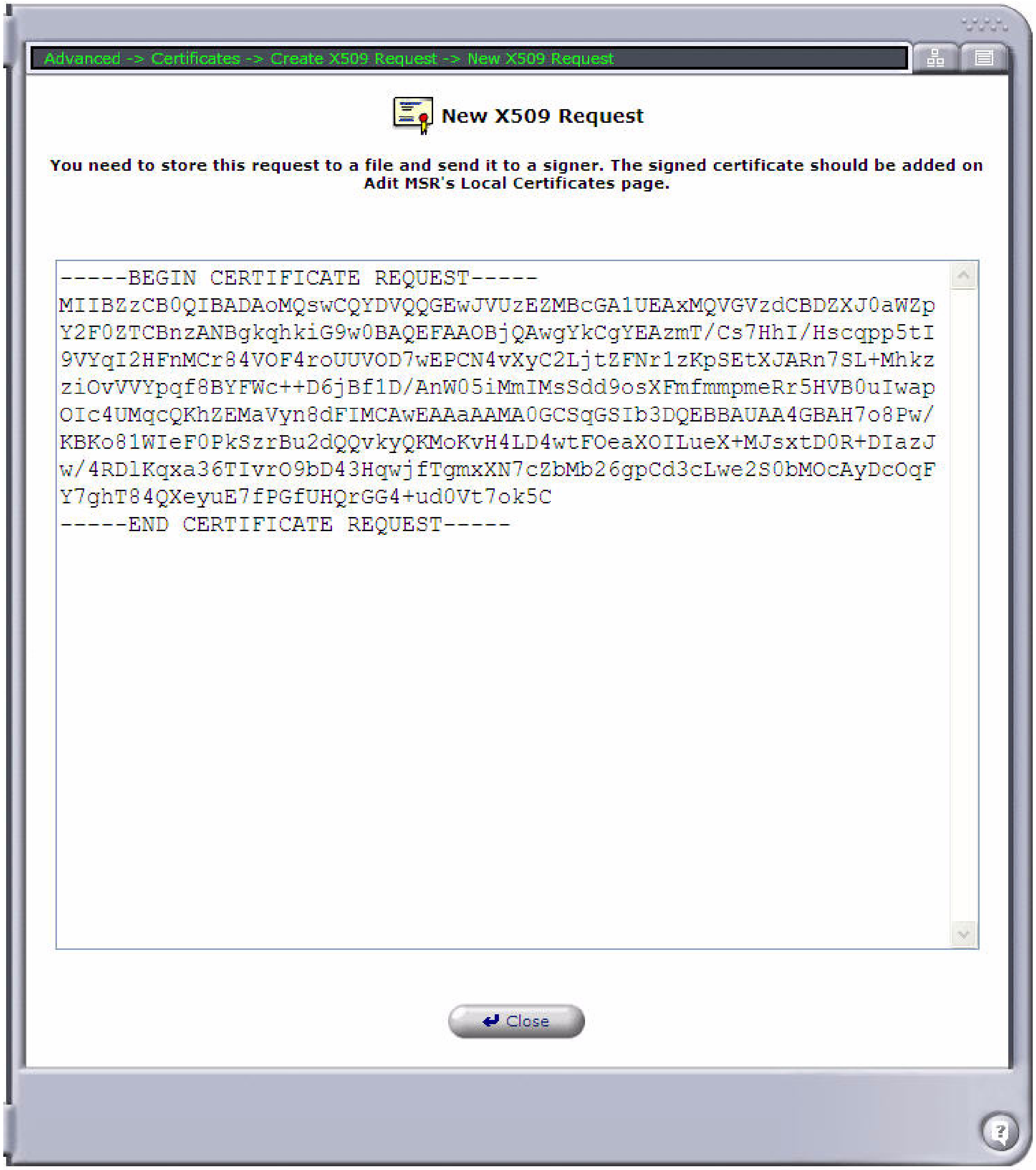
Create X509 Request

Certification Request (in PKCS #10 format)

Certificate Name:	
Subject:	
Organization:	
State:	
Country:	United States

3. Fill in your current information and select the **Generate** button.
Note: It may take a minute or so to get the certificate, and you may need to refresh the window.

4. Copy and store the exact contents of the certificate to a file, and send it to a CA for signing.



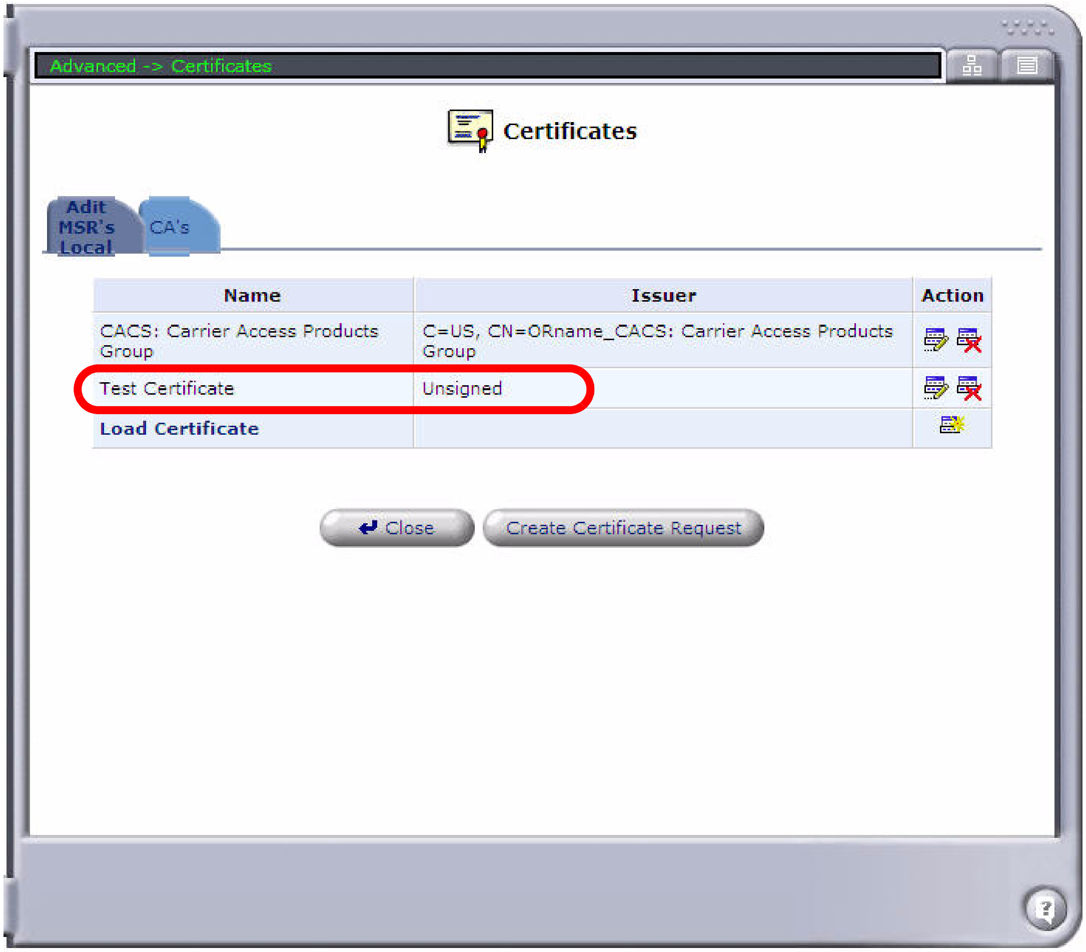
Advanced -> Certificates -> Create X509 Request -> New X509 Request

New X509 Request

You need to store this request to a file and send it to a signer. The signed certificate should be added on Adit MSR's Local Certificates page.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBZzCB0QIBADAoMQswCQYDVQQGEwJVUzEZMBcGA1UEAxMQVGVzdCBDZXJ0aWZp
Y2F0ZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzmT/Cs7HhI/Hscqpp5tI
9VYqI2HFnMCr84VOF4roUUVOD7wEPCN4vXyC2LjtZFNr1zKpSEtXJARn7SL+Mhkz
ziOvVVYpqf8BYFWc++D6jBf1D/AnW05iMmIMsSdd9osXFmfmmpmeRr5HVB0uIwap
OIc4UMqcQKhZEMaVyn8dFIMCAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GBAH7o8Pw/
KBKo81WIeF0PkSzrBu2dQQvkyQKMoKvH4LD4wtFOeaXOILueX+MJsxtD0R+DIazJ
w/4RDlKqxa36TIvrO9bD43HqwjfTgmxXN7cZbMb26gpCd3cLwe2S0bMOcAyDcOqF
Y7ghT84QXeyuE7fPGfUHQrGG4+ud0Vt7ok5C
-----END CERTIFICATE REQUEST-----
```

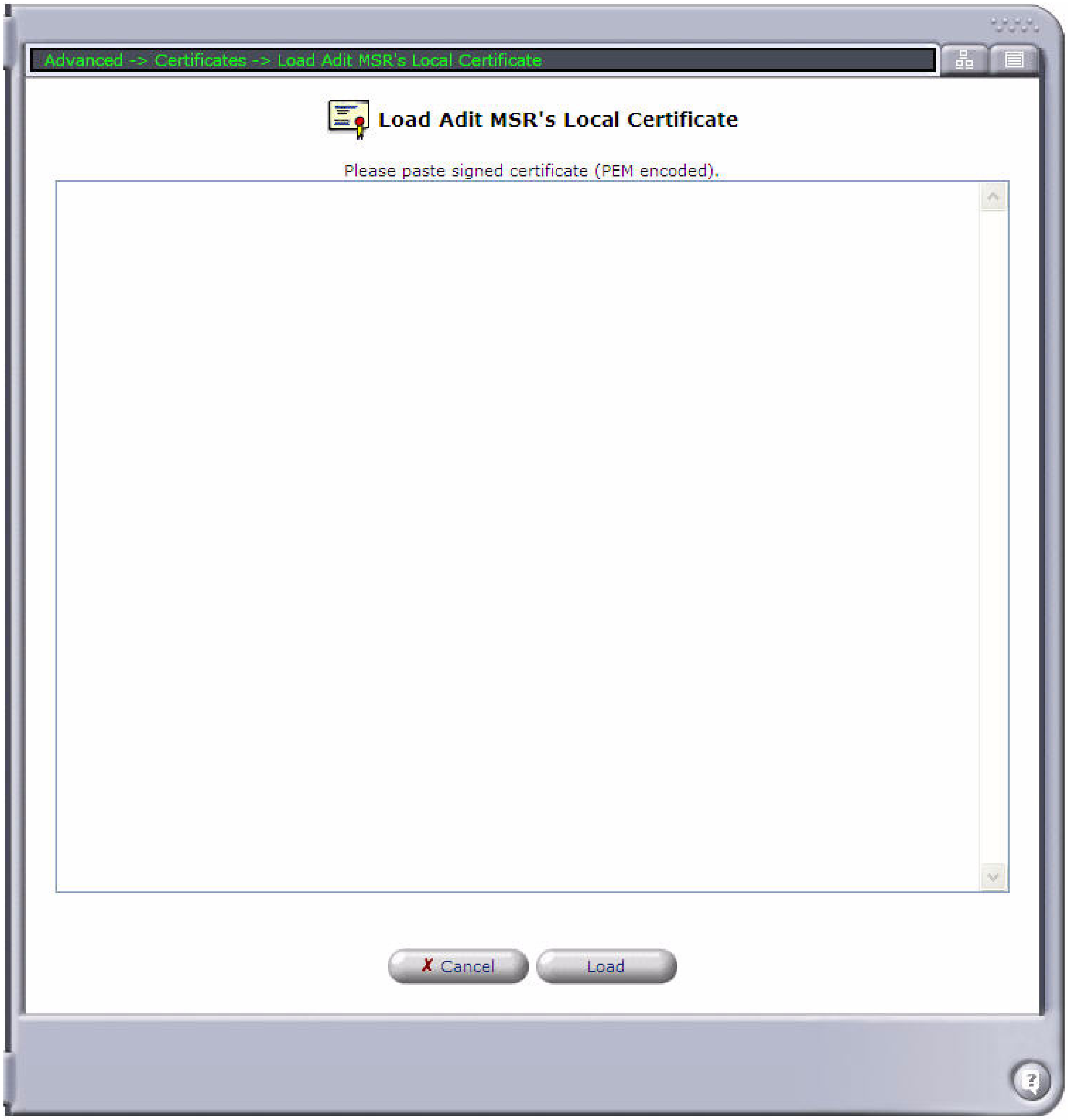
5. Select the **Close** button. The Certificates window appears, listing the certificate as **Unsigned**.



Name	Issuer	Action
CACS: Carrier Access Products Group	C=US, CN=ORname_CACS: Carrier Access Products Group	
Test Certificate	Unsigned	
Load Certificate		

6. After receiving the signed certificate from the CA, select **Load Certificate**.

7. Paste the signed certificate.



Advanced -> Certificates -> Load Adit MSR's Local Certificate

Load Adit MSR's Local Certificate

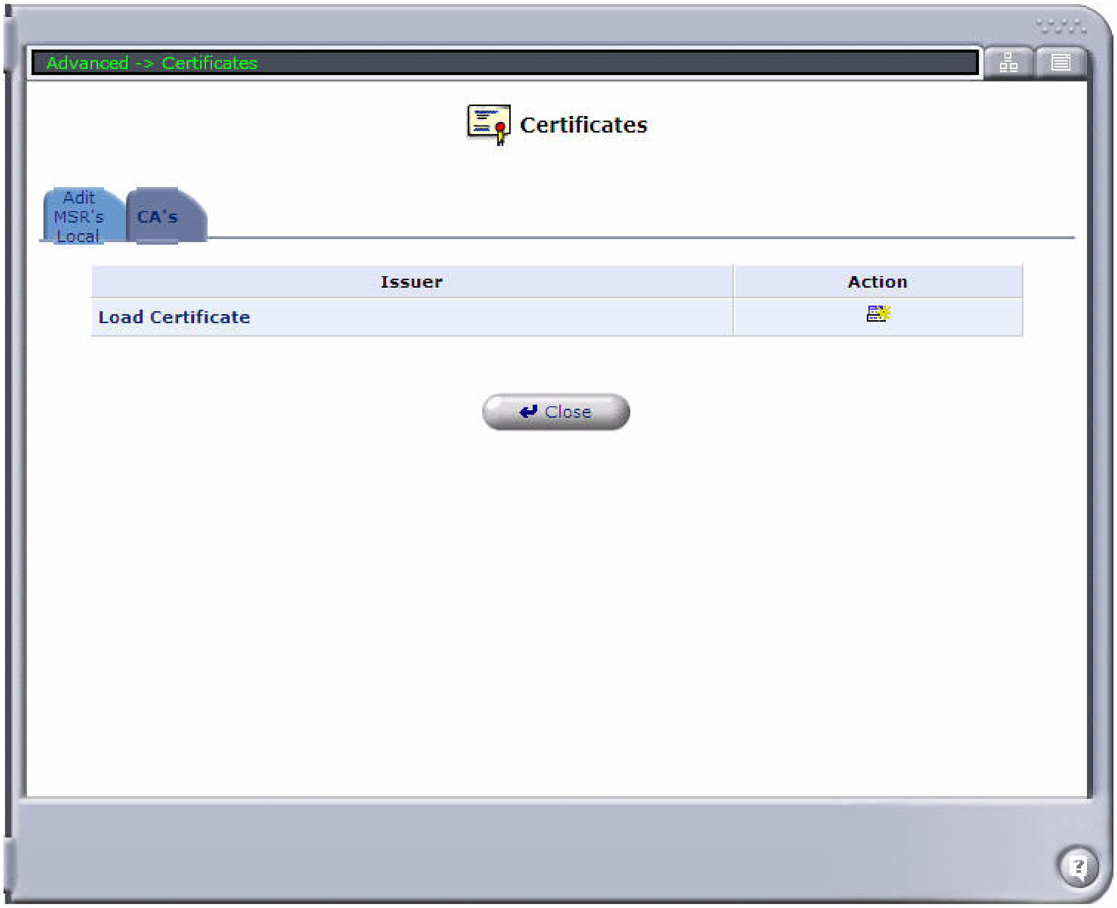
Please paste signed certificate (PEM encoded).

8. Select the **Load** button. The Certificates window appears, displaying the name and issuer of the certificate.

Registering the CA's Certificate

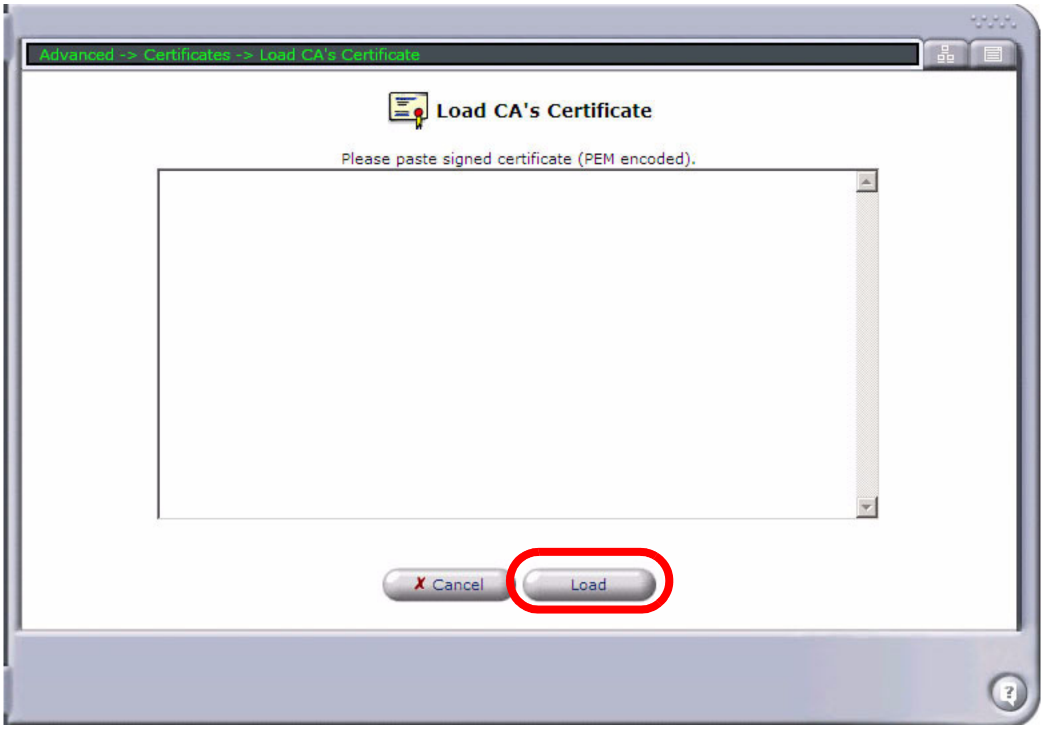
After receiving the signed certificate from the CA:

1. Select the **CA's** tab on the Advanced/Certificates window.



Issuer	Action
Load Certificate	

2. Select **Load Certificate**, and paste the CA's certificate into the window.



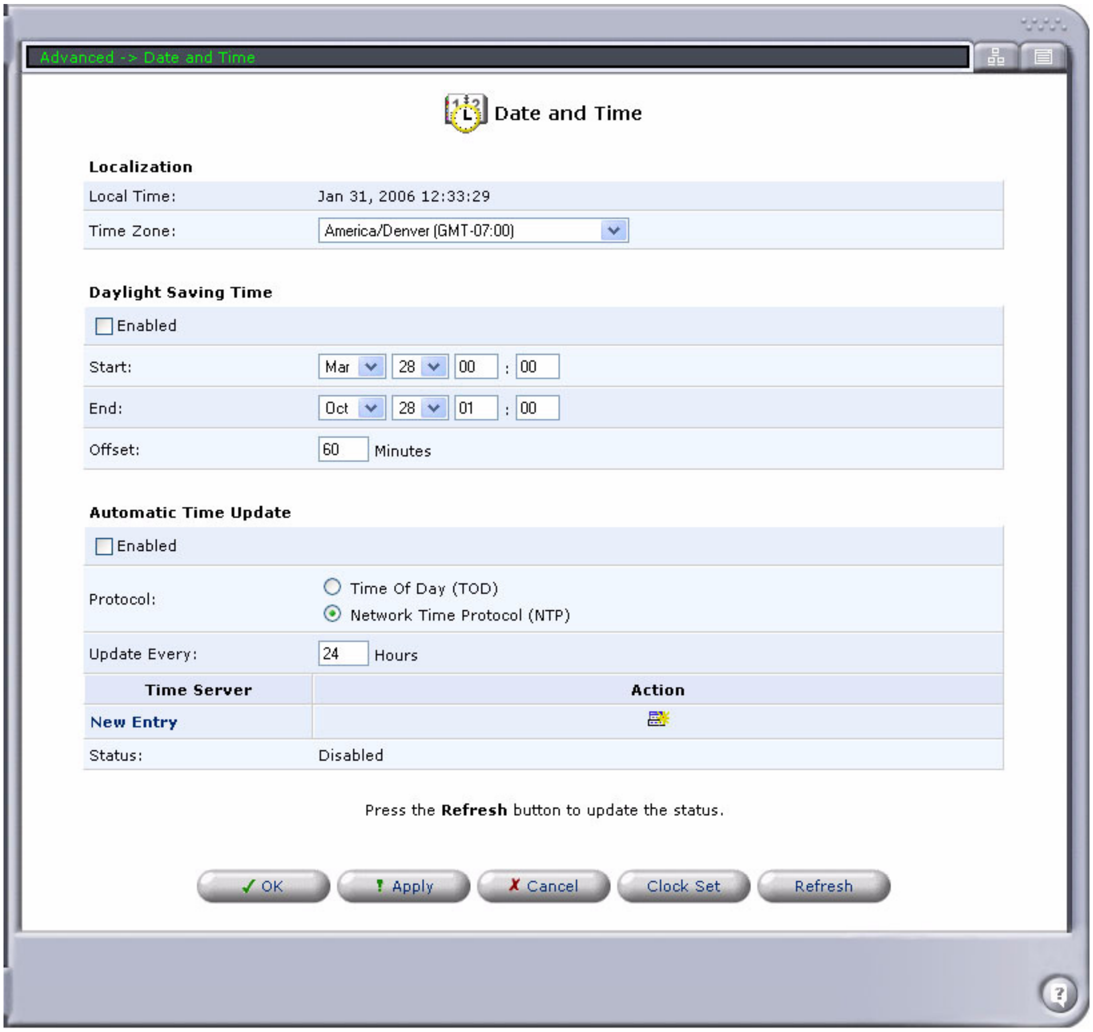
Advanced -> Certificates -> Load CA's Certificate
Load CA's Certificate
Please paste signed certificate (PEM encoded).
✗ Cancel
Load

3. Select the **Load** button to register the signed Certificate. The Certificates window appears, displaying the name and issuer of the certificate.

Date and Time

This window allows the user to configure the date and time parameters for the unit.

NOTE: By default, Time of Day management for the MSR is provided by the Adit 600 controller. Use the settings in this window for the MSR only if you are using NTP or another time service and need to manually adjust the time due to a loss of contact with the server.



Date and Time

Localization

Local Time:	Jan 31, 2006 12:33:29
Time Zone:	America/Denver (GMT-07:00)

Daylight Saving Time

□ Enabled	
Start:	Mar 28 00 : 00
End:	Oct 28 01 : 00
Offset:	60 Minutes

Automatic Time Update

□ Enabled	
Protocol:	○ Time Of Day (TOD) ● Network Time Protocol (NTP)
Update Every:	24 Hours

Time Server	Action
New Entry	
Status:	Disabled

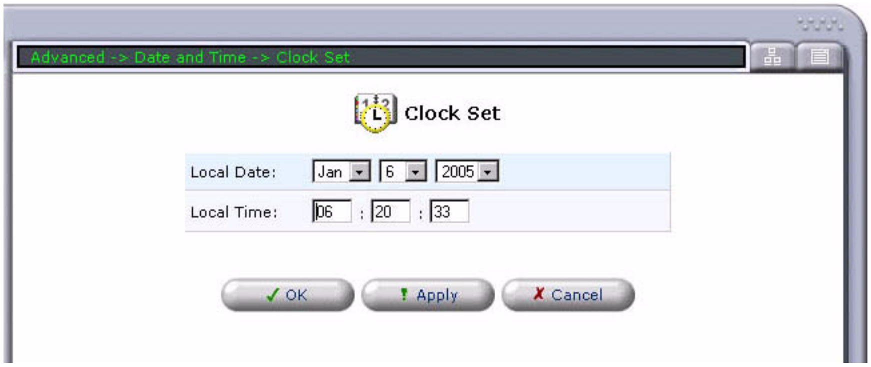
Press the **Refresh** button to update the status.

Setting the Date and Time

1. Select **Advanced/ Date and Time**.
2. Set the Time Zone of this unit from the **Time Zone** pulldown menu.
3. Set **Daylight Saving Time** as necessary:

Field	Definition
Enabled	Check box to enable Daylight Saving Time.
Start	Set the date and time when Daylight Saving starts.
End	Set the date and time when Daylight Saving ends.
Offset	Set the Daylight Saving Time offset.

4. To configure the current date, select the **Clock Set** button. Enter the current system date and time, then click **OK**.



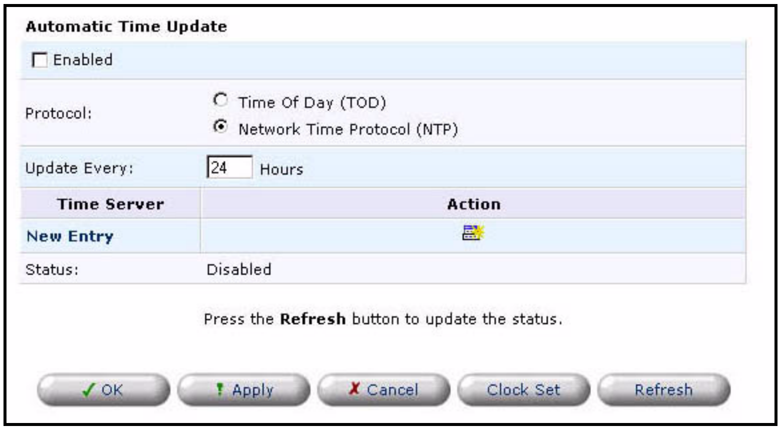
Advanced -> Date and Time -> Clock Set

Clock Set

Local Date: Jan 6 2005

Local Time: 06 : 20 : 33

5. Configure **Automatic Time Update** (bottom of window) as desired.



Automatic Time Update

☐ Enabled

Protocol: ○ Time Of Day (TOD) ● Network Time Protocol (NTP)

Update Every: 24 Hours

Time Server	Action
New Entry	

Status: Disabled

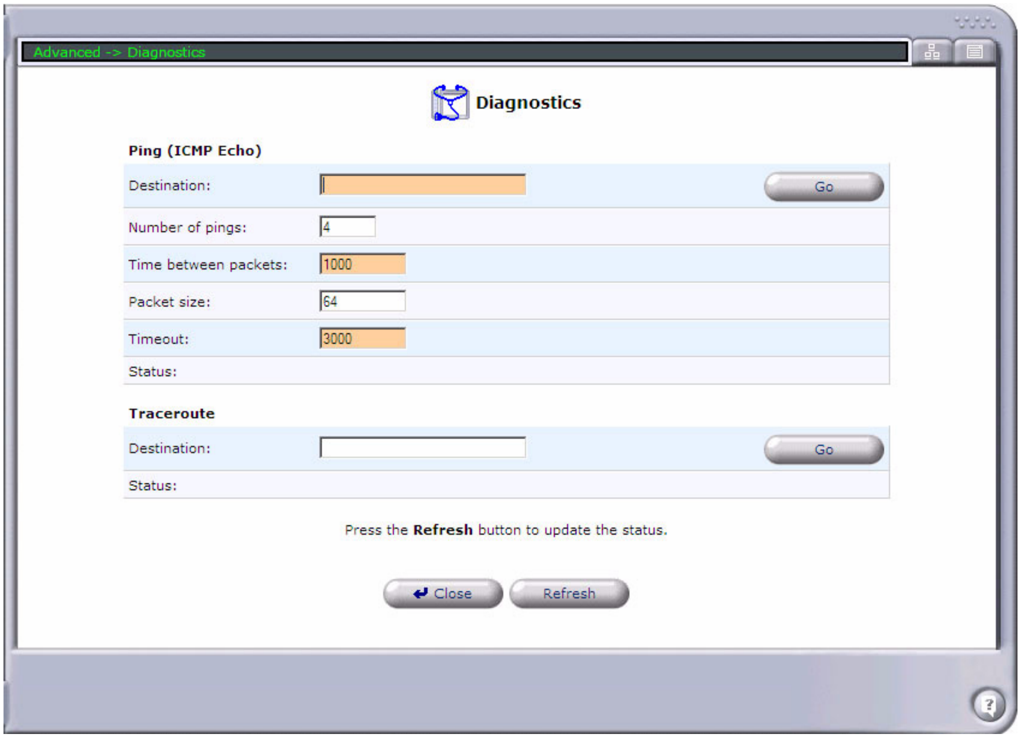
Press the **Refresh** button to update the status.

Field	Definition
Enabled	Check box to enable the Automatic Time Update.
Protocol	Select the protocol to be used to perform the time update. **Time of Day** - Retrieves the time from the TOD server (defined in the Time Server field below). **Network Time Protocol -** Retrieves the time from the network (Network Time Server defined in the Time Server field below).
Update Every	Range 1-480 hours.
Time Server	Select **New Entry** and enter the IP Address or domain name of the Time Server.
Status	Displays the current status of the Automatic Time Update.

Diagnostics

The Diagnostics window allows the user to test network connectivity using the following methods:

- Ping an IP address and view the statics
- Perform a Traceroute



Diagnostics

Ping (ICMP Echo)

Destination:	
Number of pings:	4
Time between packets:	1000
Packet size:	64
Timeout:	3000
Status:	

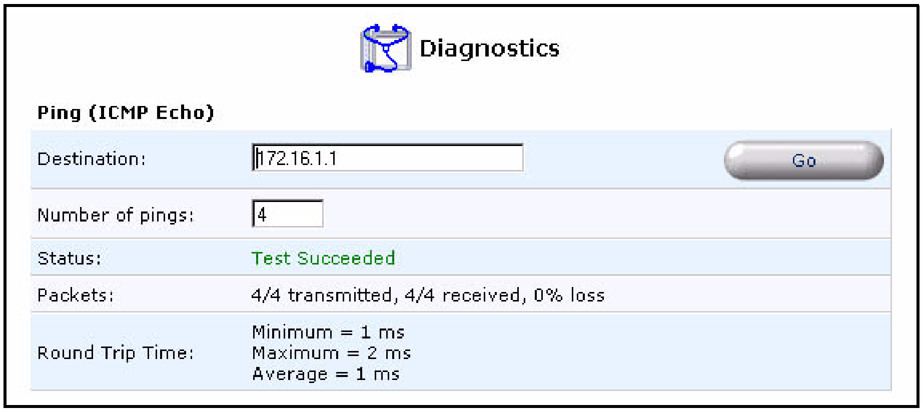
Traceroute

Destination:	
Status:	

Press the **Refresh** button to update the status.

Pinging an IP Address

1. Select **Advanced/ Diagnostics**.
2. Enter the IP address in the **Ping/Destination** field.
3. Select the **Go** button. The results of the Ping will be displayed.



Diagnostics

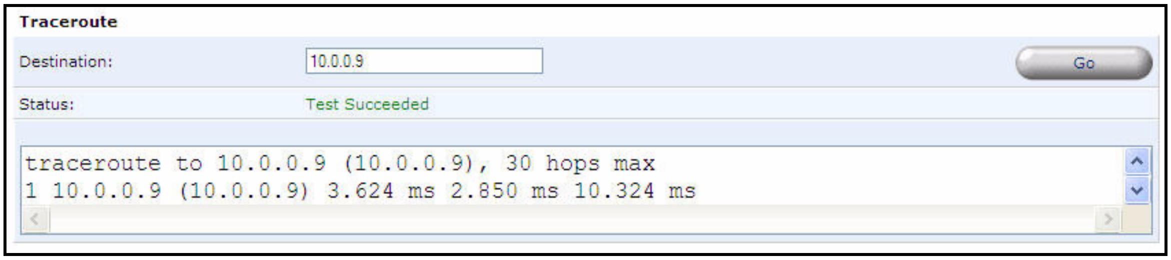
Ping (ICMP Echo)

Destination:	172.16.1.1
Number of pings:	4
Status:	Test Succeeded
Packets:	4/4 transmitted, 4/4 received, 0% loss

Round Trip Time:	Minimum = 1 ms
	Maximum = 2 ms
	Average = 1 ms

Performing a Traceroute

1. Select **Advanced/ Diagnostics**.
2. Enter the IP address in the **Traceroute/Destination** field.
3. Select the **Go** button. The results of the Traceroute will be displayed.



Traceroute

Destination:	10.0.0.9
Status:	Test Succeeded

```
traceroute to 10.0.0.9 (10.0.0.9), 30 hops max
1 10.0.0.9 (10.0.0.9) 3.624 ms 2.850 ms 10.324 ms
```

DNS Static Entries

The Domain Naming System (DNS) provides a service that translates domain names into IP addresses and vice versa. The Adit's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network, the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address.

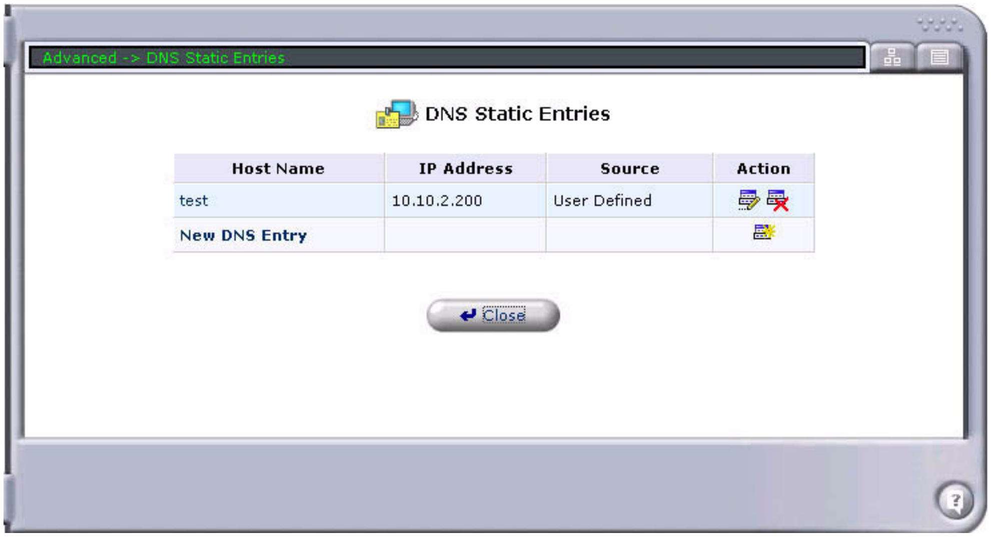
Additional features of the Adit's DNS:

- Shares a common database of domain names/IP addresses with the DHCP server
- Supports multiple subnets within the LAN simultaneously
- Automatically appends a domain name to unqualified names
- Allows new domain names to be added to the database using the Adit's Web-based Management
- Permits a computer to have multiple host names
- Permits a host name to have multiple IPs (if a host has multiple network cards)

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

Viewing the DNS Table

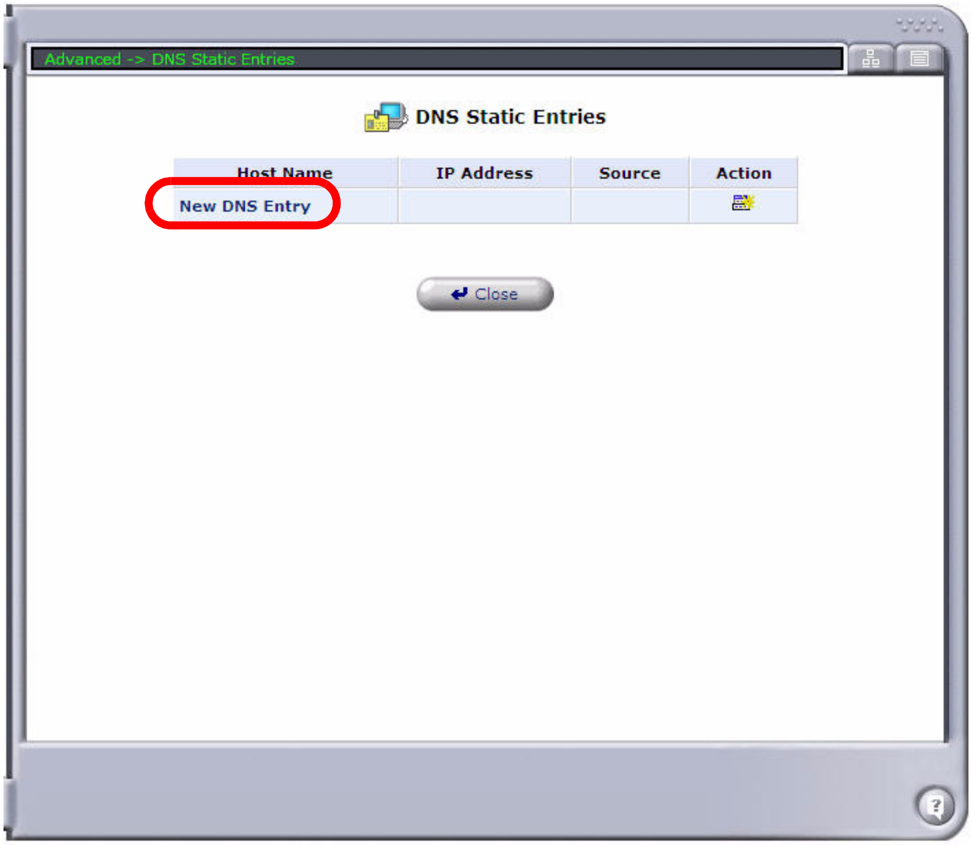
1. Select **Advanced/ DNS Static Entries**.



Host Name	IP Address	Source	Action
test	10.10.2.200	User Defined	✎ ✗
New DNS Entry			✚

Adding a New Entry to the DNS Table

1. Select **Advanced/ DNS Static Entries**.
2. Select **New DNS Entry**.

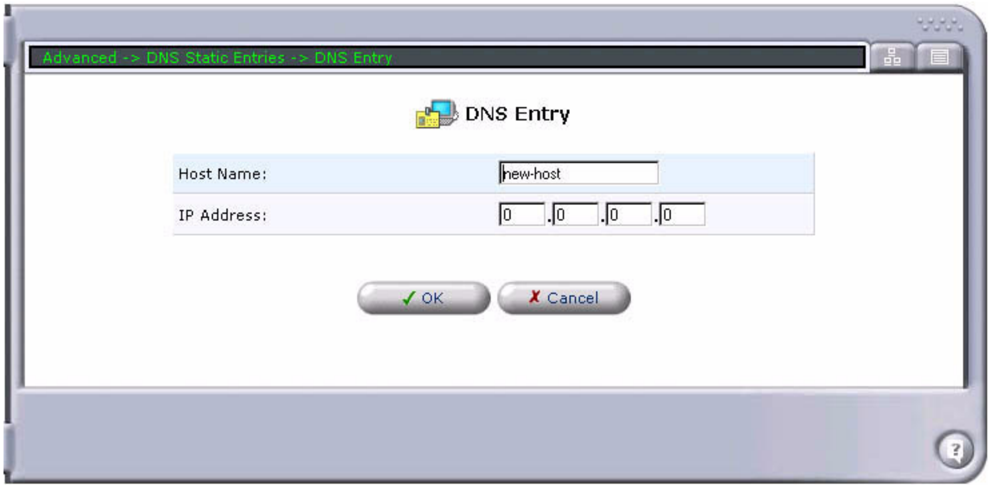


Advanced -> DNS Static Entries

DNS Static Entries

Host Name	IP Address	Source	Action
New DNS Entry			

3. Enter the computer’s **Host Name** and **IP Address**.



Advanced -> DNS Static Entries -> DNS Entry

DNS Entry

Host Name:	new-host
IP Address:	0 .0 .0 .0

4. Select **OK**. The new DNS entry is displayed in the DNS Static Entries table.

Modifying an Entry in the DNS Table

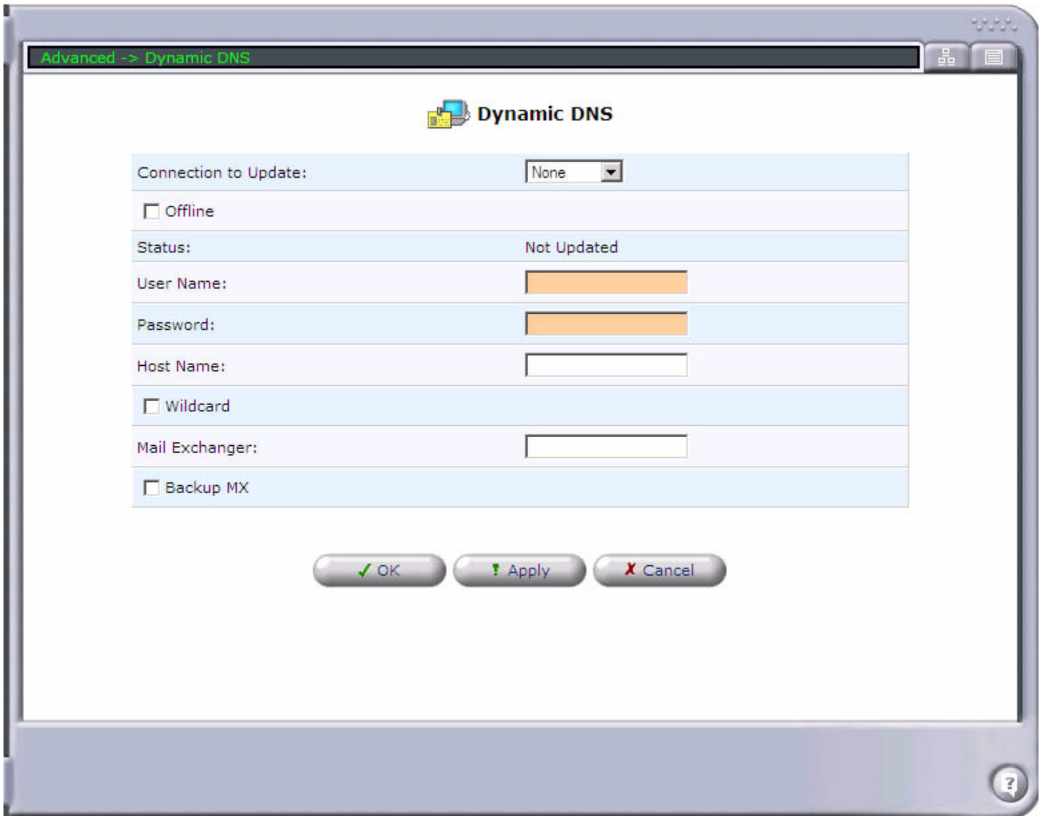
1. Select **Advanced/ DNS Static Entries**.
2. Select an entry on the list to modify.
3. The DNS Entry window appears. Modify the **Host Name** and **IP Address**, as needed.
4. Select **OK**. The modified DNS entry is displayed in the DNS Static Entries table.

NOTE: An entry can be deleted by selecting the **Action/Delete** button.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static host name, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, while maintaining a constant domain name. Each time the IP address provided by your ISP changes, the DNS database will change accordingly to reflect the change in IP address. In this way, even though a domain name's IP address will change often, your domain name will still be accessible.

To be able to use the Dynamic DNS feature you must open a DDNS account, free of charge, at http://www.dyndns.org/account/create.html. When applying for an account, you will need to specify a user name and password. For more information regarding Dynamic DNS, please refer to http://www.dyndns.org.



Advanced -> Dynamic DNS

Dynamic DNS

Connection to Update:	None
□ Offline	
Status:	Not Updated
User Name:	
Password:	
Host Name:	
□ Wildcard	
Mail Exchanger:	
□ Backup MX	

Using Dynamic DNS

1. Select **Advanced/ Dynamic DNS**.
2. Specify the Dynamic DNS operating parameters:

Field	Definition
Connection to Update	Select the connection to be used for the update from the pulldown menu.
Offline	Select the checkbox to work offline.
Status	The status field displays relevant information regarding the information exchange between the Adit and DDNS. The Manual Update button invokes a manual update of the DDNS parameters. It is not advisable to frequently update the DDNS parameters manually, since this may cause unneccessary traffic on the DDNS servers.
User Name	Enter your Dyndns user name.
Password	Enter you Dyndns password.
Host Name	Enter a subdomain name, and select a suffix from the domain combo-box to define your host name. The Name may not contain spaces. Only letters, digits, dash (-), underscore (_) or a dot (.). These special characters (- _ .) may not appear at the beginning or at the end of a name. The maximum length of a label (text between two dots) is 63.
Wildcard	This allows a user to update DNS records for a specific sub-domain, therefore not updating all sub-domains.
Mail Exchanger	Enter your mail exchange server address, to redirect all E-mails arriving at your Dyndns address to your mail server.
Backup MX	Backup mail exchanger.

3. Select **Apply** or **OK** to save the configuration.

IP Address Distribution (DHCP)

The Adit's DHCP server makes it possible to easily add computers that are configured as DHCP clients to the network. It provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to them.

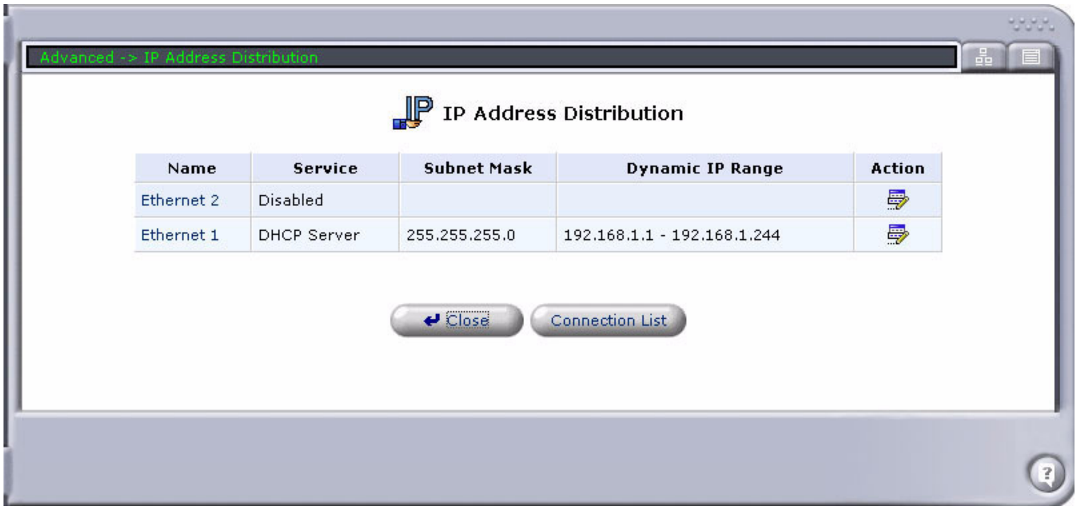
The DHCP-based autoconfiguration feature provides a method of updating the Adit's firmware and configuration automatically. This is accomplished by querying a DHCP server in the boot sequence, then using the data provided to download firmware and configuration files, and then rebooting if there are changes that need to take effect.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as "taken". At this point the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease, it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration, it can send a release message to the DHCP server, which will then make the IP address available for use by others.

Summary of Services

To view a summary of the services currently being provided by the DHCP server, select **Advanced/ IP Address Distribution**.



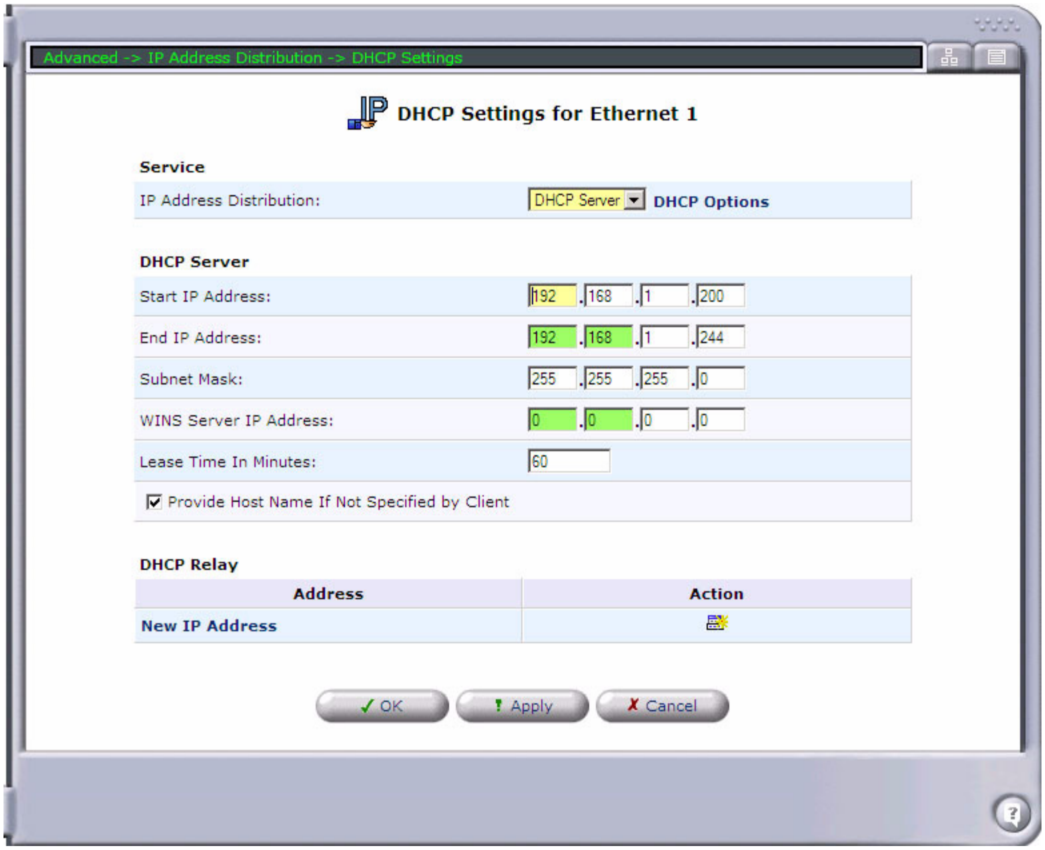
Name	Service	Subnet Mask	Dynamic IP Range	Action
Ethernet 2	Disabled			✎
Ethernet 1	DHCP Server	255.255.255.0	192.168.1.1 - 192.168.1.244	✎

NOTE: If a device is listed as **Disabled** in the **Status** column, DHCP services are not being provided to hosts connected to the network through that device. This means that the Adit will not assign IP addresses to these computers. This may be of some use when working with static IP addresses only.

Editing DHCP Server Settings

To edit the DHCP server setting for a device:

1. Select **Advanced/ IP Address Distribution**.
2. Select the interface to configure (Ethernet 1/Ethernet 2).



Advanced -> IP Address Distribution -> DHCP Settings

DHCP Settings for Ethernet 1

Service

IP Address Distribution: DHCP Server

DHCP Server

Start IP Address: 192 . 168 . 1 . 200

End IP Address: 192 . 168 . 1 . 244

Subnet Mask: 255 . 255 . 255 . 0

WINS Server IP Address: 0 . 0 . 0 . 0

Lease Time In Minutes: 60

☑ Provide Host Name If Not Specified by Client

DHCP Relay

Address	Action
New IP Address	

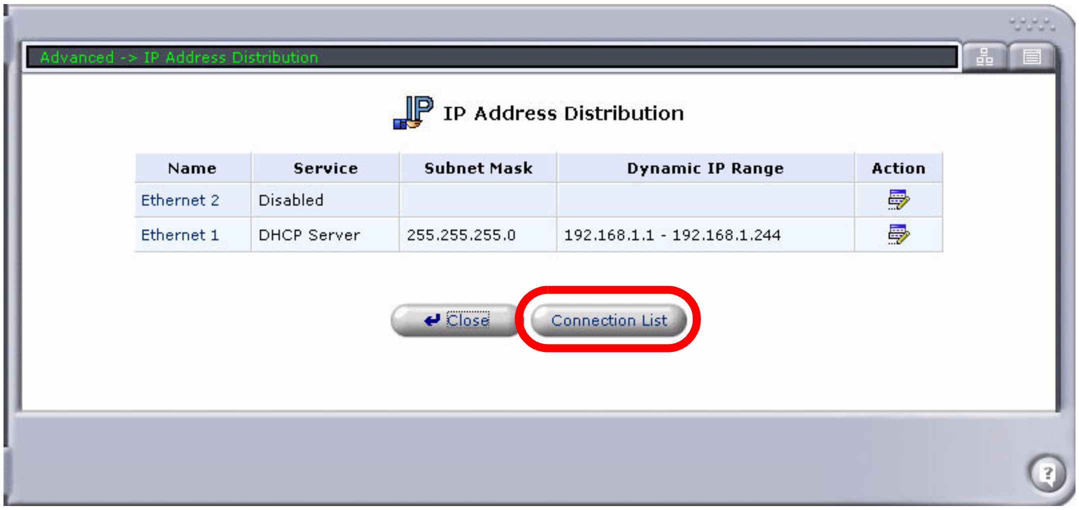
3. Edit the DHCP settings by completing the following fields:

Field	Definition
IP Address Distribution	**Disabled** - Disables DHCP. **DHCP Server** - Assigns addresses to LAN clients. **DHCP Relay** - Responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.
DHCP Server	
Start IP Address	The IP address range defines the number of hosts that may be connected to the network in this subnet. **Start** defines the first IP address that may be assigned in this subnet.
End IP Address	**End IP address** defines the last IP address in the subnet (see above).
Subnet Mask	A mask used to define the subnet an IP address belongs to.
WINS Server IP Address	Enter the WINS server IP address.
Lease Time In Minutes	The lease duration in minutes.

Field	Definition (Continued)
Provide Host Name if Not Specified by Client	If the DHCP client does not have a host name, the Adit will assign the client a default name.
DHCP Relay	
New IP Address	Opens a new window for entering an IP address.

Defining a New Connection with a Fixed IP Address

1. Select **Advanced/ IP Address Distribution**.

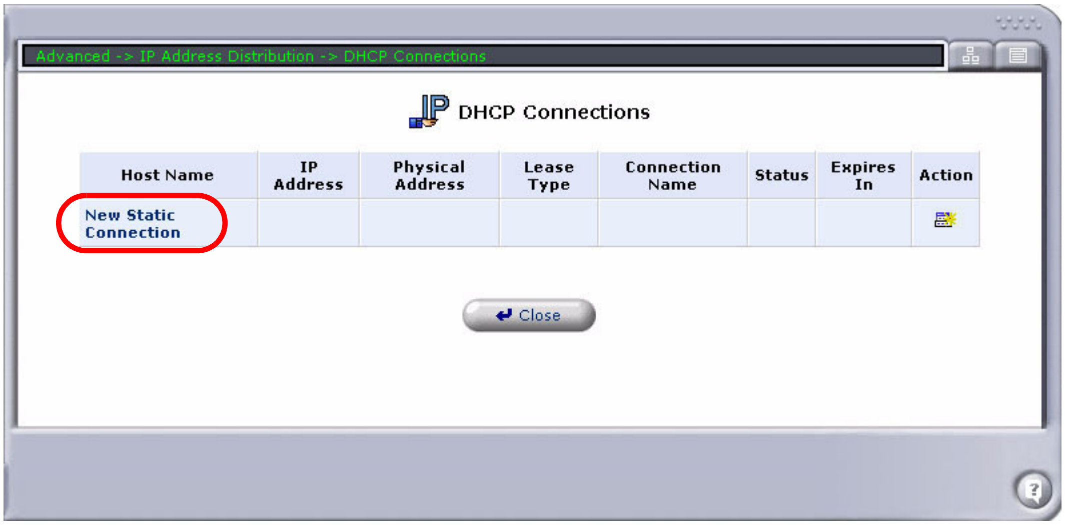


Advanced -> IP Address Distribution

IP Address Distribution

Name	Service	Subnet Mask	Dynamic IP Range	Action
Ethernet 2	Disabled			
Ethernet 1	DHCP Server	255.255.255.0	192.168.1.1 - 192.168.1.244	

2. Select the **Connection List** button.

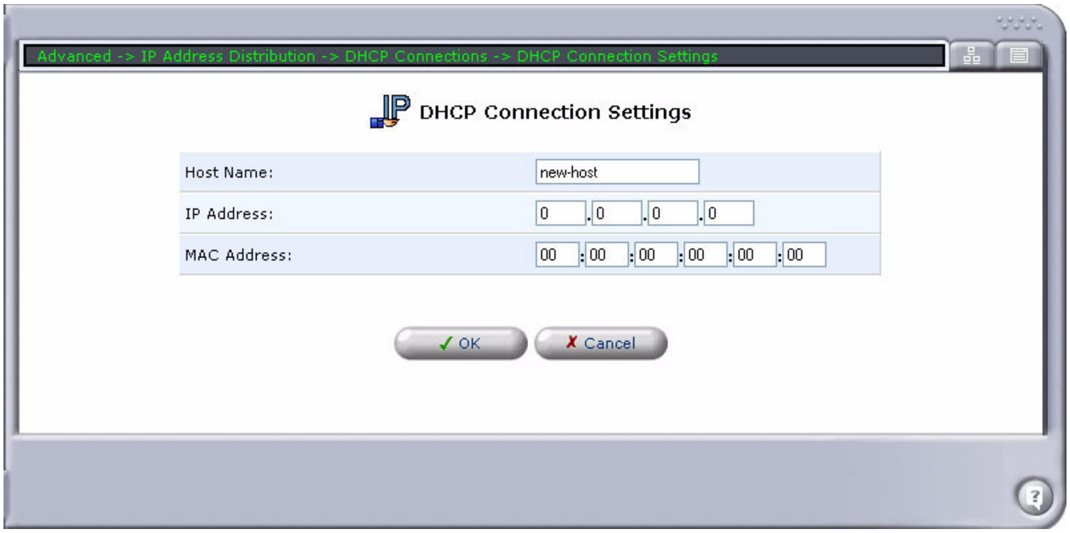


Advanced -> IP Address Distribution -> DHCP Connections

DHCP Connections

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
New Static Connection							

3. Select **New Static Connection**.



Advanced -> IP Address Distribution -> DHCP Connections -> DHCP Connection Settings

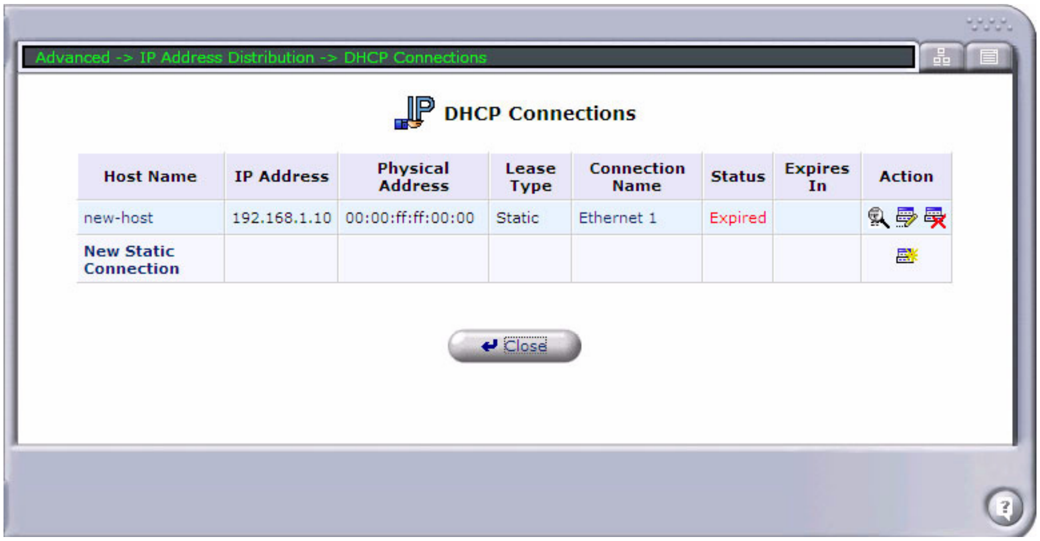
DHCP Connection Settings

Host Name:	new-host
IP Address:	0 . 0 . 0 . 0
MAC Address:	00 : 00 : 00 : 00 : 00 : 00

4. Enter the host information in the following fields:

Field	Definition
Host Name	Enter the host name for this connection.
IP Address	Enter a fixed IP address to assign to the computer.
MAC Address	Enter the MAC address of the computer's network card.

5. Select **OK** to save the configuration. The DHCP Connections window will display the Static Connection.



Advanced -> IP Address Distribution -> DHCP Connections

DHCP Connections

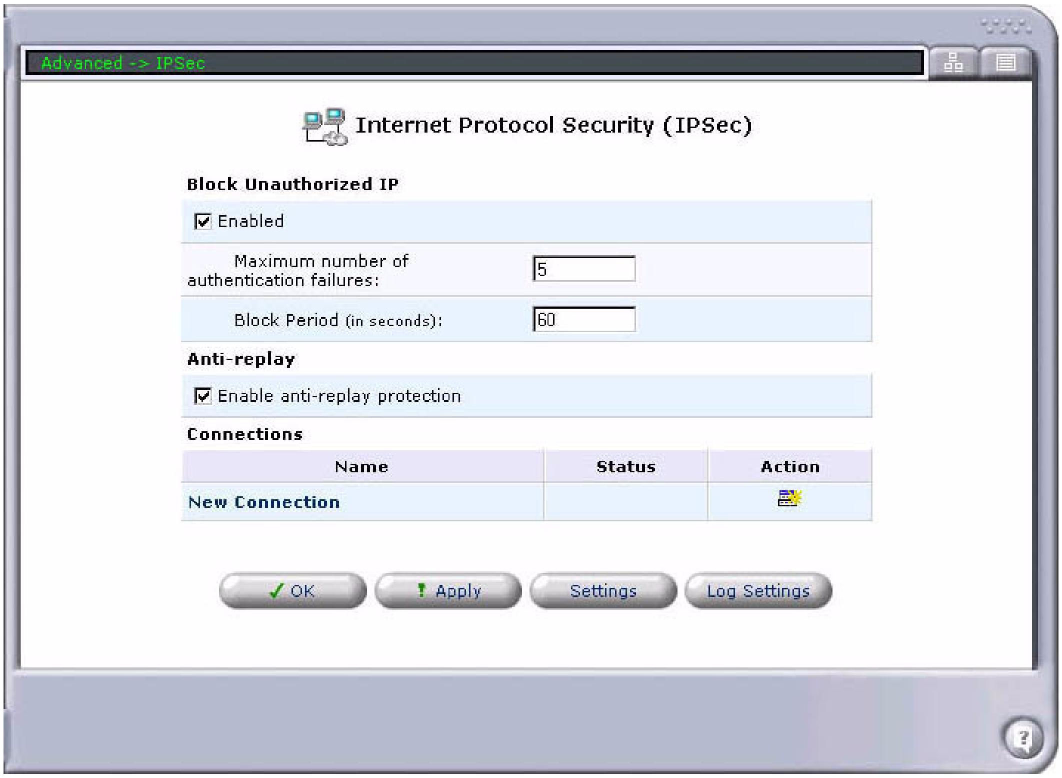
Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
new-host	192.168.1.10	00:00:ff:ff:00:00	Static	Ethernet 1	Expired		
New Static Connection							

IPSec (IP Security)

IPSec (IP security) is a standard for securing IP communications by encrypting and/or authenticating all IP packets. IPSec provides security at the network level.

The Internet Protocol Security (IPSec) window allows display/modification of IPSec settings:

- General IPSec settings
- Key management settings
- Log settings
- Advanced IPSec Connection settings



Advanced -> IPSec

Internet Protocol Security (IPSec)

Block Unauthorized IP

☑ Enabled

Maximum number of authentication failures: 5

Block Period (in seconds): 60

Anti-replay

☑ Enable anti-replay protection

Connections

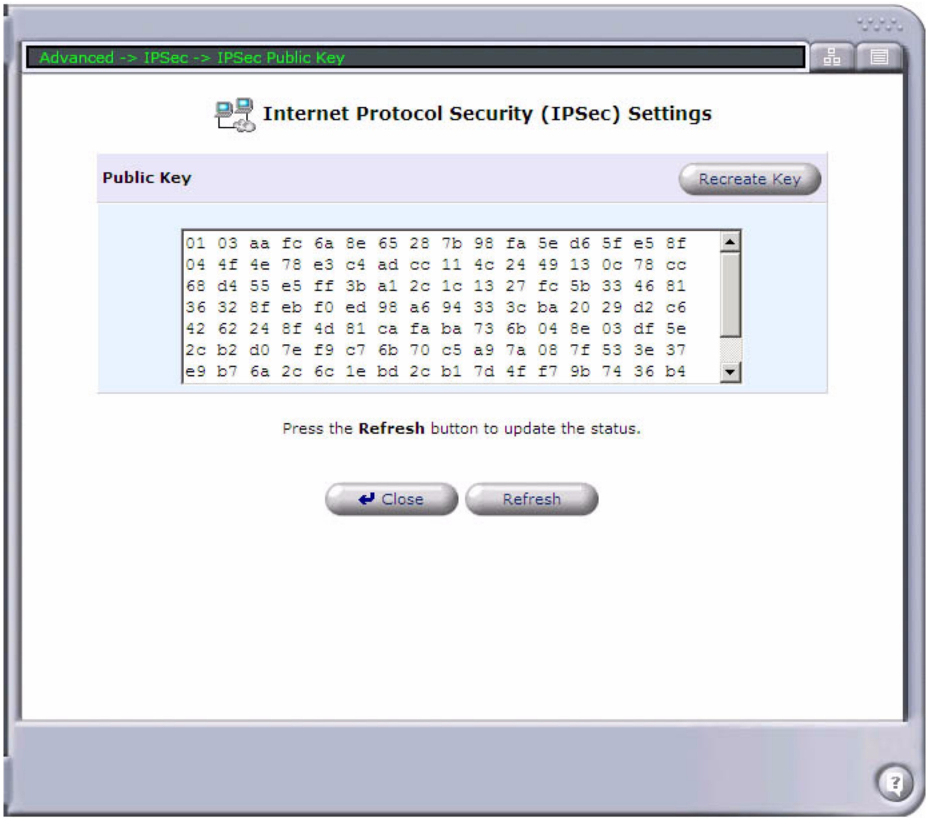
Name	Status	Action
New Connection		

General IPSec Settings

Field	Definition
Block Unauthorized IP	When an IP address fails to register with IPSec connection, it can be blocked for a set amount of time by the firewall.
Enabled	Checked box enables the blocking of unauthorized IP access.
Maximum number or authentication failures	Maximum number of failures before a block takes effect. Range 0 - 2147483647 failures.
Block Period	Sets the number of seconds for the IP address to be blocked. Range 0 - 2147483647 seconds.
Anti-Replay	
Enable anti-replay protection	Anti-Replay is a security service where the receiver can reject old or duplicate packets to protect itself against replay attacks. IPSec provides this optional service by use of a sequence number combined with the use of data authentication. PIX Firewall IPSec provides this service whenever it provides the data authentication service, except in the following: The service is not available for manually established security associations (security associations established by manual configuration and not by IKE).
Connections	
New Connection	Creates a new secured connection. The user is guided through a series of windows to configure this connection.

Key Management

1. Select **Advanced/ IPSec**.
2. Select the **Settings** button.


Advanced -> IPSec -> IPSec Public Key
Internet Protocol Security (IPSec) Settings
Public Key
Recreate Key

```
01 03 aa fc 6a 8e 65 28 7b 98 fa 5e d6 5f e5 8f
04 4f 4e 78 e3 c4 ad cc 11 4c 24 49 13 0c 78 cc
68 d4 55 e5 ff 3b a1 2c 1c 13 27 fc 5b 33 46 81
36 32 8f eb f0 ed 98 a6 94 33 3c ba 20 29 d2 c6
42 62 24 8f 4d 81 ca fa ba 73 6b 04 8e 03 df 5e
2c b2 d0 7e f9 c7 6b 70 c5 a9 7a 08 7f 53 3e 37
e9 b7 6a 2c 6c 1e bd 2c b1 7d 4f f7 9b 74 36 b4
```

Press the **Refresh** button to update the status.

3. The **Settings** window displays the Adit's public key. If necessary, you can copy the public key from this window.

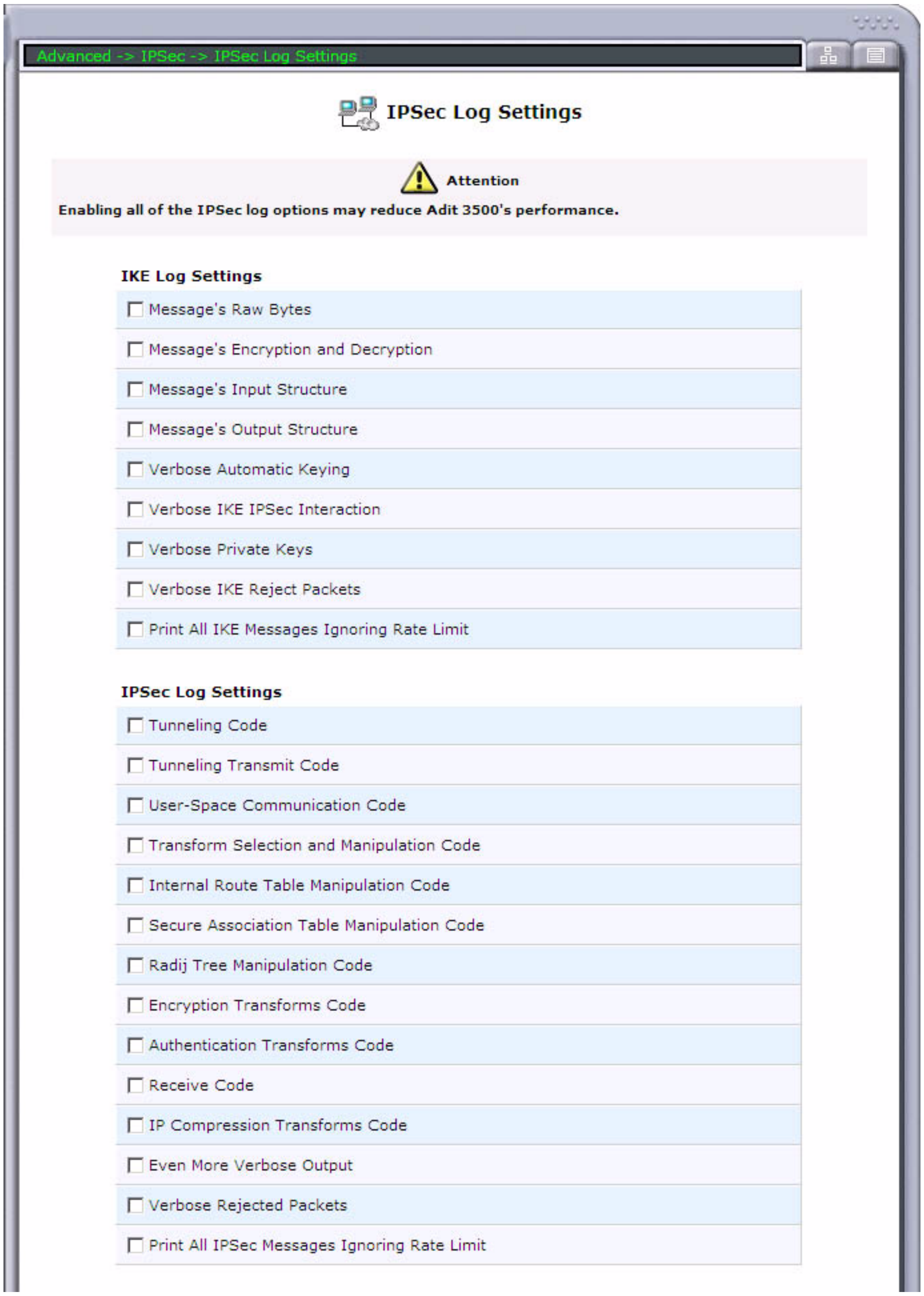
Field	Definition
Recreate Key (button)	Recreate the public key.
Refresh (button)	Refresh the public key displayed.

Log Settings

Use the IPSec Log Settings window to specify the type of information to be displayed in the IPSec Log.

NOTE: The IPSec log is displayed in the System Log (**System Monitoring/System Log**). Events can also be forwarded to another location.

1. Select **Advanced/ IPSec**.
2. Select the **Log Settings** button.



Advanced -> IPSec -> IPSec Log Settings

IPSec Log Settings

Attention

Enabling all of the IPSec log options may reduce Adit 3500's performance.

IKE Log Settings

- □ Message's Raw Bytes
- □ Message's Encryption and Decryption
- □ Message's Input Structure
- □ Message's Output Structure
- □ Verbose Automatic Keying
- □ Verbose IKE IPSec Interaction
- □ Verbose Private Keys
- □ Verbose IKE Reject Packets
- □ Print All IKE Messages Ignoring Rate Limit

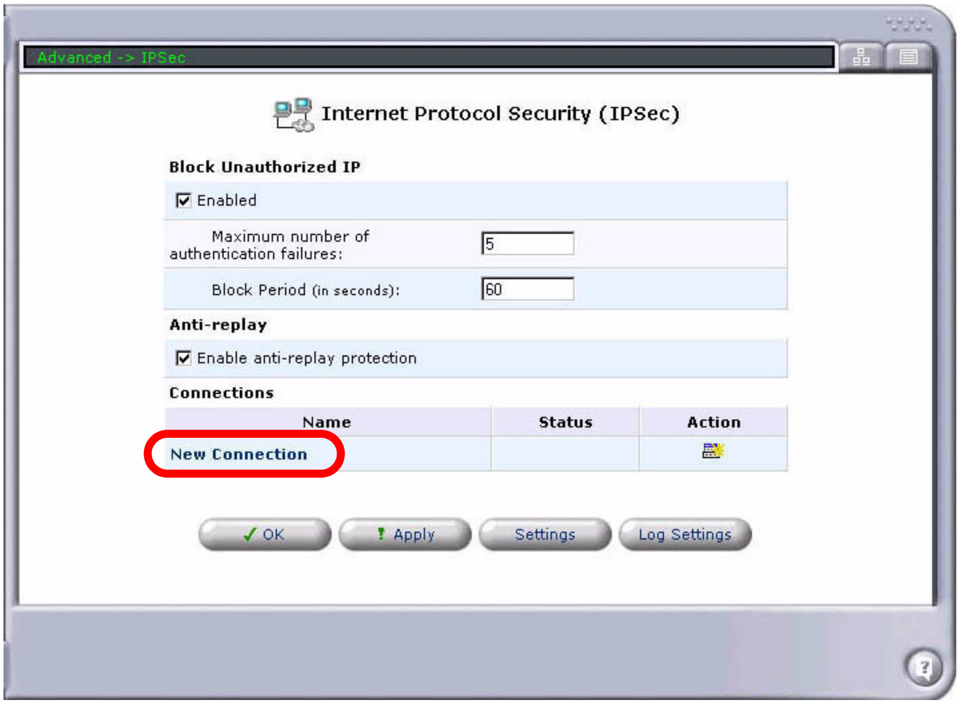
IPSec Log Settings

- □ Tunneling Code
- □ Tunneling Transmit Code
- □ User-Space Communication Code
- □ Transform Selection and Manipulation Code
- □ Internal Route Table Manipulation Code
- □ Secure Association Table Manipulation Code
- □ Radij Tree Manipulation Code
- □ Encryption Transforms Code
- □ Authentication Transforms Code
- □ Receive Code
- □ IP Compression Transforms Code
- □ Even More Verbose Output
- □ Verbose Rejected Packets
- □ Print All IPSec Messages Ignoring Rate Limit

3. Select the check boxes next to the information you would like recorded in the IPSec log. Click **OK**.

Creating a New Secured Connection

1. Select **New Connection** on the Internet Protocol Security (IPSec) window.



Internet Protocol Security (IPSec)

Block Unauthorized IP

☑ Enabled

Maximum number of authentication failures:	5
Block Period (in seconds):	60

Anti-replay

☑ Enable anti-replay protection

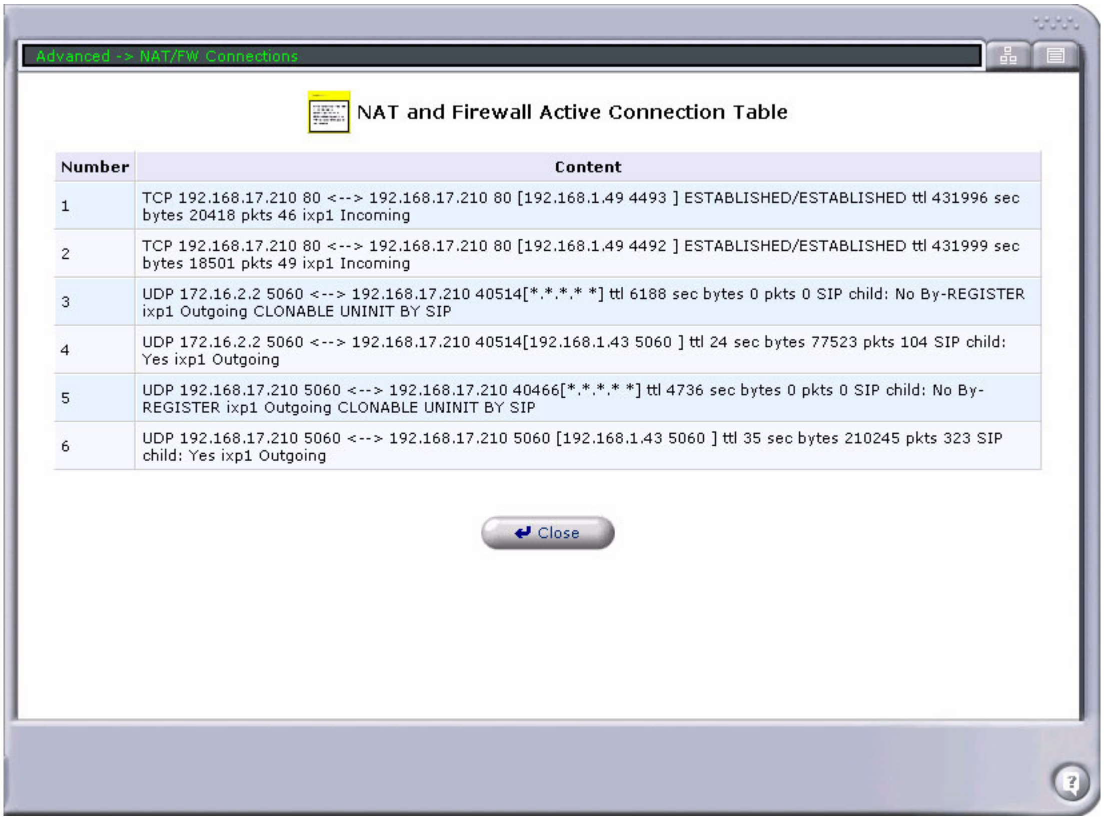
Connections

Name	Status	Action
New Connection		

2. Follow the instructions provided in the series of screens presented.

NAT/FW Connections

The NAT Firewall Connections table displays all active NAT and Firewall connections.



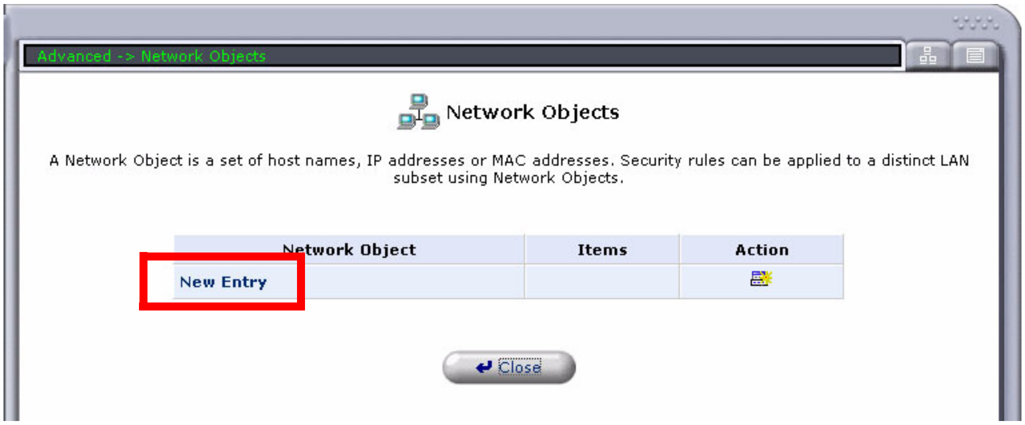
NAT and Firewall Active Connection Table

Number	Content
1	TCP 192.168.17.210 80 <--> 192.168.17.210 80 [192.168.1.49 4493] ESTABLISHED/ESTABLISHED ttl 431996 sec bytes 20418 pkts 46 ixp1 Incoming
2	TCP 192.168.17.210 80 <--> 192.168.17.210 80 [192.168.1.49 4492] ESTABLISHED/ESTABLISHED ttl 431999 sec bytes 18501 pkts 49 ixp1 Incoming
3	UDP 172.16.2.2 5060 <--> 192.168.17.210 40514[*.*.*.* *] ttl 6188 sec bytes 0 pkts 0 SIP child: No By-REGISTER ixp1 Outgoing CLONABLE UNINIT BY SIP
4	UDP 172.16.2.2 5060 <--> 192.168.17.210 40514[192.168.1.43 5060] ttl 24 sec bytes 77523 pkts 104 SIP child: Yes ixp1 Outgoing
5	UDP 192.168.17.210 5060 <--> 192.168.17.210 40466[*.*.*.* *] ttl 4736 sec bytes 0 pkts 0 SIP child: No By-REGISTER ixp1 Outgoing CLONABLE UNINIT BY SIP
6	UDP 192.168.17.210 5060 <--> 192.168.17.210 5060 [192.168.1.43 5060] ttl 35 sec bytes 210245 pkts 323 SIP child: Yes ixp1 Outgoing

Network Objects

The Network Objects window will create a Network Object, which is a set of host names, IP address or MAC addresses. Network Objects allow security rules to be applied to a distinct LAN subset.

1. Select **Advanced/ Network Objects**.
2. Select **New Entry**.



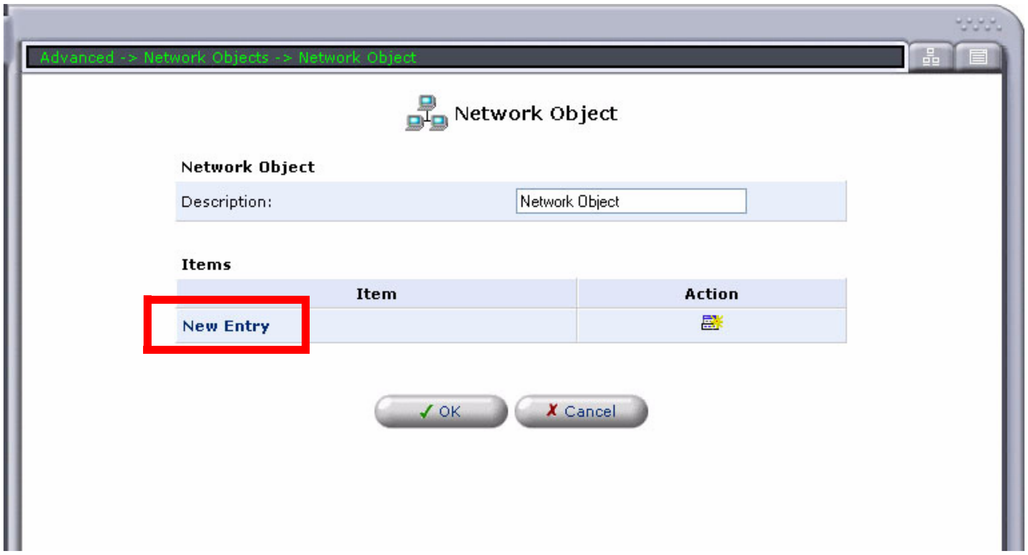
Advanced -> Network Objects

Network Objects

A Network Object is a set of host names, IP addresses or MAC addresses. Security rules can be applied to a distinct LAN subset using Network Objects.

Network Object	Items	Action
New Entry		

3. Name the **Network Object** in the **Description** field.
4. Select **New Entry** under Items..



Advanced -> Network Objects -> Network Object

Network Object

Network Object

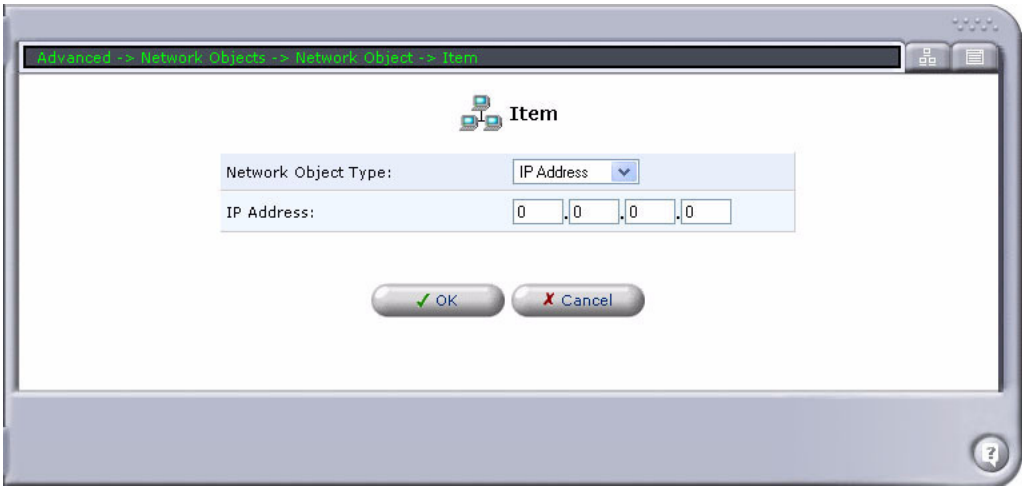
Description:	Network Object

Items

Item	Action
New Entry	

5. Set the following fields:

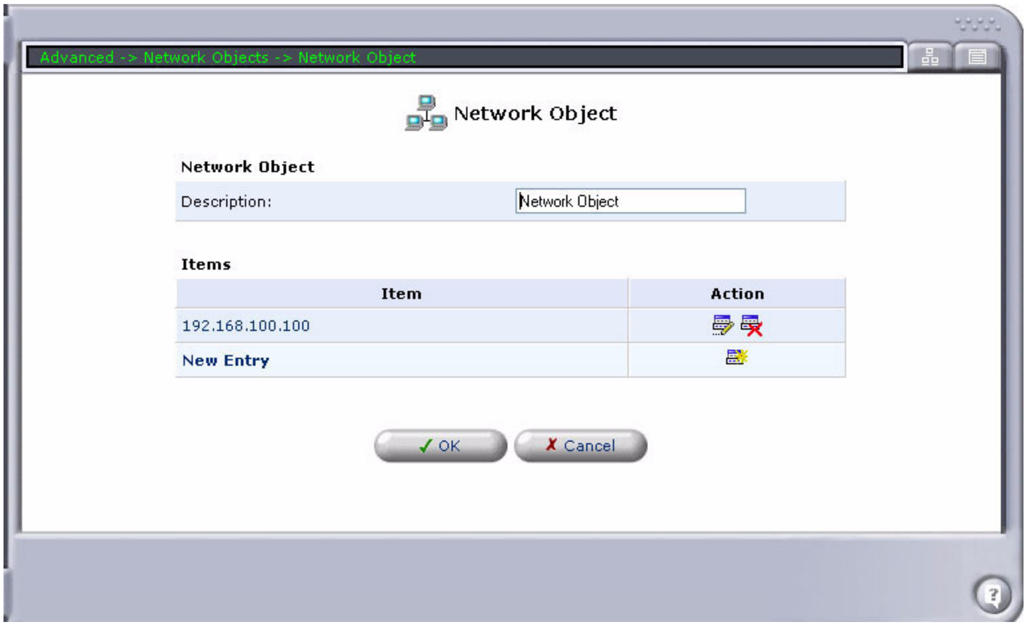
Field	Definition
Network Object Type	**IP Address** - Enter the IP address of the Network Object.
	MAC Address - Enter the MAC address of the Network Object.
	Host Name - enter the Host Name of the Network Object.



Network Object Type: IP Address

IP Address: 0 .0 .0 .0

6. Click **OK**. The newly created Network Object appears in the Network Objects table.



Network Object

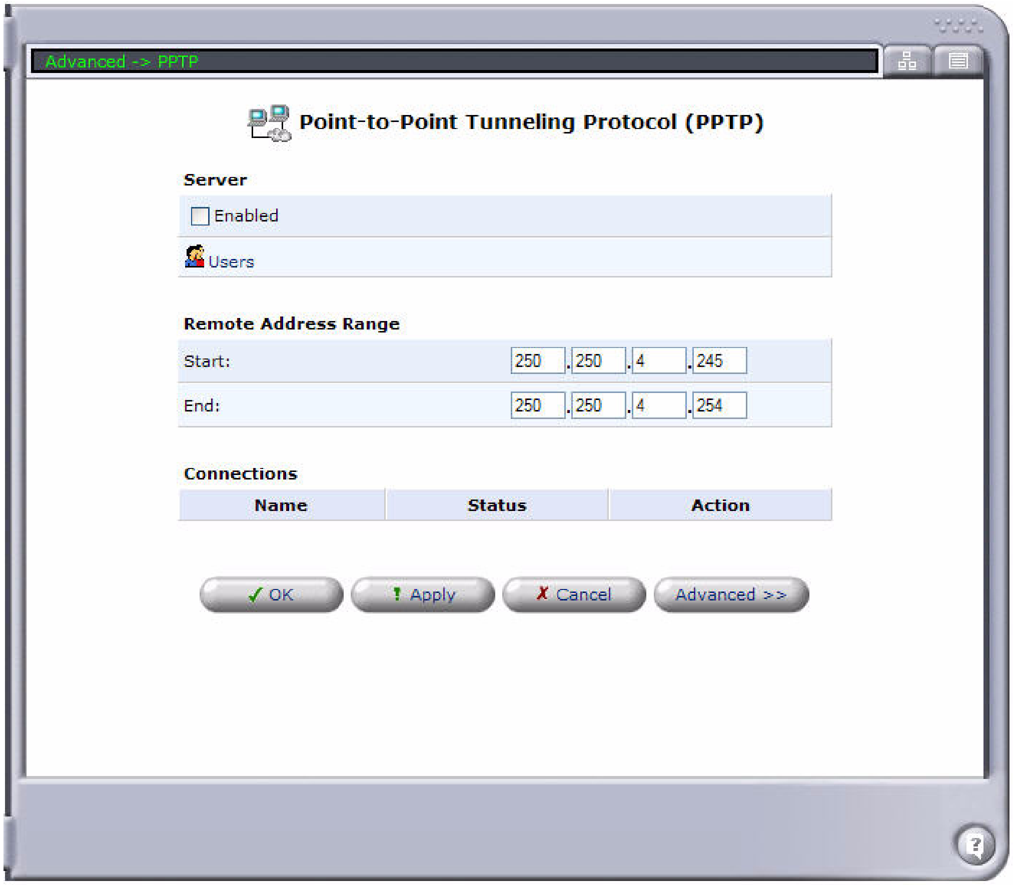
Description: Network Object

Items

Item	Action
192.168.100.100	
New Entry	

PPTP (Point-to-Point Tunneling Protocol)

The Adit can be configured as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.



Advanced -> PPTP

Point-to-Point Tunneling Protocol (PPTP)

Server

☐ Enabled

Users

Remote Address Range

Start:	250 . 250 . 4 . 245
End:	250 . 250 . 4 . 254

Connections

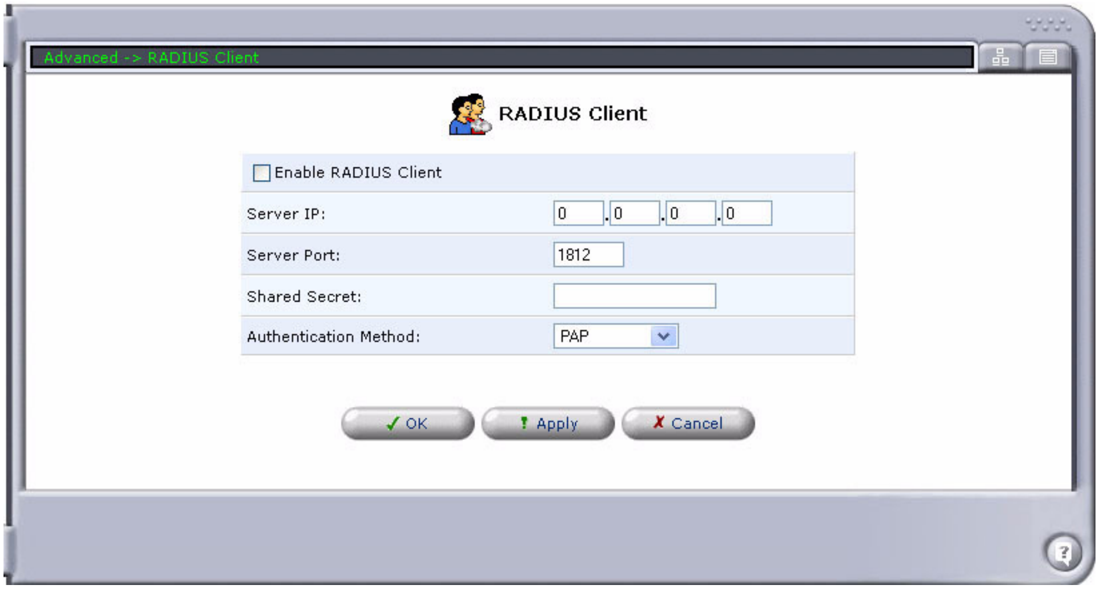
Name	Status	Action

RADIUS Client

For authentication to function, the client's transmission must go through the Adit and reach the back-end server that performs the actual authentication. The wireless client contacts the access point, which in-turn, communicates with the RADIUS (Remote Authentication Dial-in User Service) server. The RADIUS server verifies the client's credentials to determine whether the device is authorized to connect to the LAN. If the RADIUS server accepts the client, the server responds by exchanging data with the Adit, including security keys for subsequent encrypted sessions.

Configuring RADIUS

1. Select **Advanced/ RADIUS Client.**



Advanced -> RADIUS Client

RADIUS Client

☐ Enable RADIUS Client

Server IP:	0 . 0 . 0 . 0
Server Port:	1812
Shared Secret:	
Authentication Method:	PAP

2. Set the following fields:

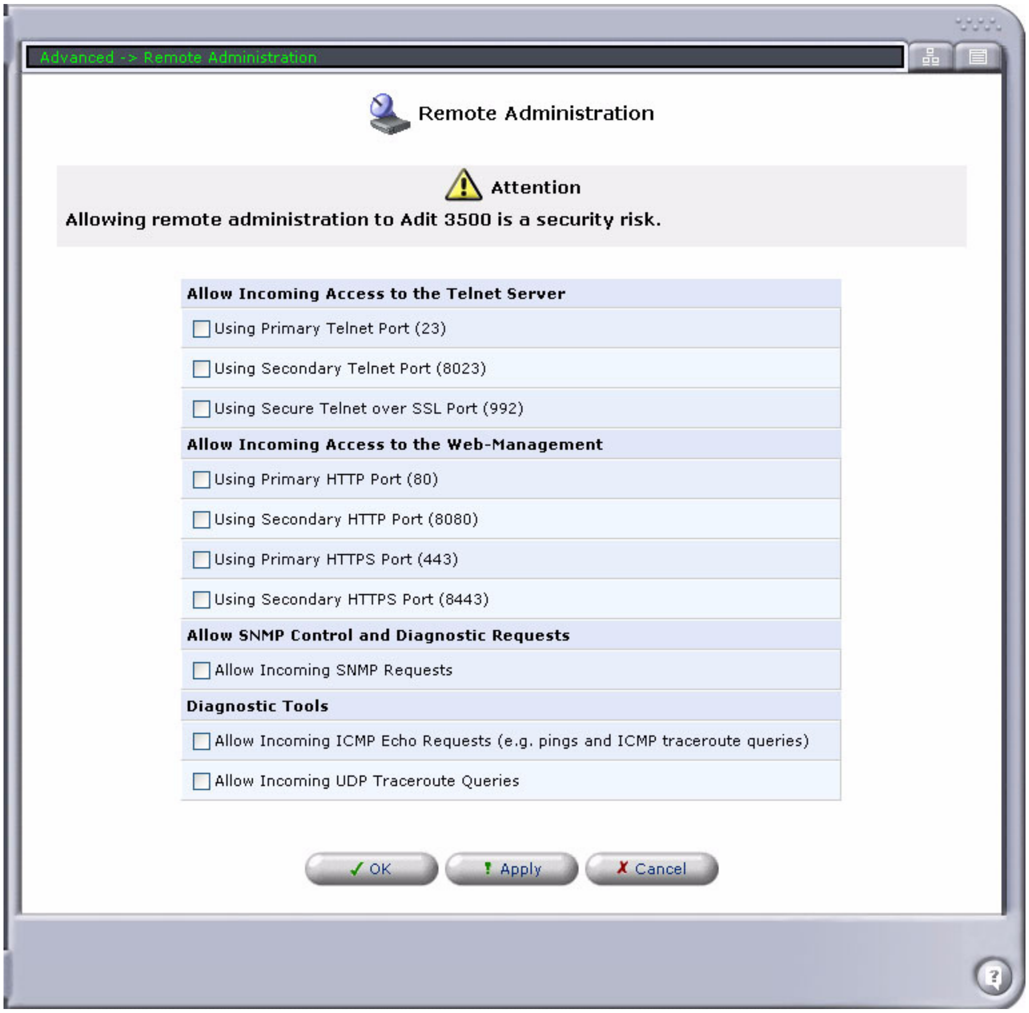
Field	Definition
Enable RADIUS Client	Enables RADIUS client authentication.
Server IP	Enter the RADIUS server's IP address.
Server Port	Enter the RADIUS server's port.
Shared Secret	Enter your shared secret password, up to 8 characters.
Authentication Method	From the pulldown menu select the method: **PAP** - Unencrypted Password **CHAP** - Challenge Handshake Authentication **MS-CHAP** - Microsoft CHAP **MS-CHAPv2** - Microsoft CHAP Version 2

Remote Administration

In it's default state, the Adit locks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may wish to enable certain services that grant remote users administrative privileges in your network.

Configuring Remote Administration Services

1. Select **Advanced/ Remote Administration**.



Remote Administration

Attention

Allowing remote administration to Adit 3500 is a security risk.

Allow Incoming Access to the Telnet Server

□ Using Primary Telnet Port (23)

□ Using Secondary Telnet Port (8023)

□ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the Web-Management

□ Using Primary HTTP Port (80)

□ Using Secondary HTTP Port (8080)

□ Using Primary HTTPS Port (443)

□ Using Secondary HTTPS Port (8443)

Allow SNMP Control and Diagnostic Requests

□ Allow Incoming SNMP Requests

Diagnostic Tools

□ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

□ Allow Incoming UDP Traceroute Queries

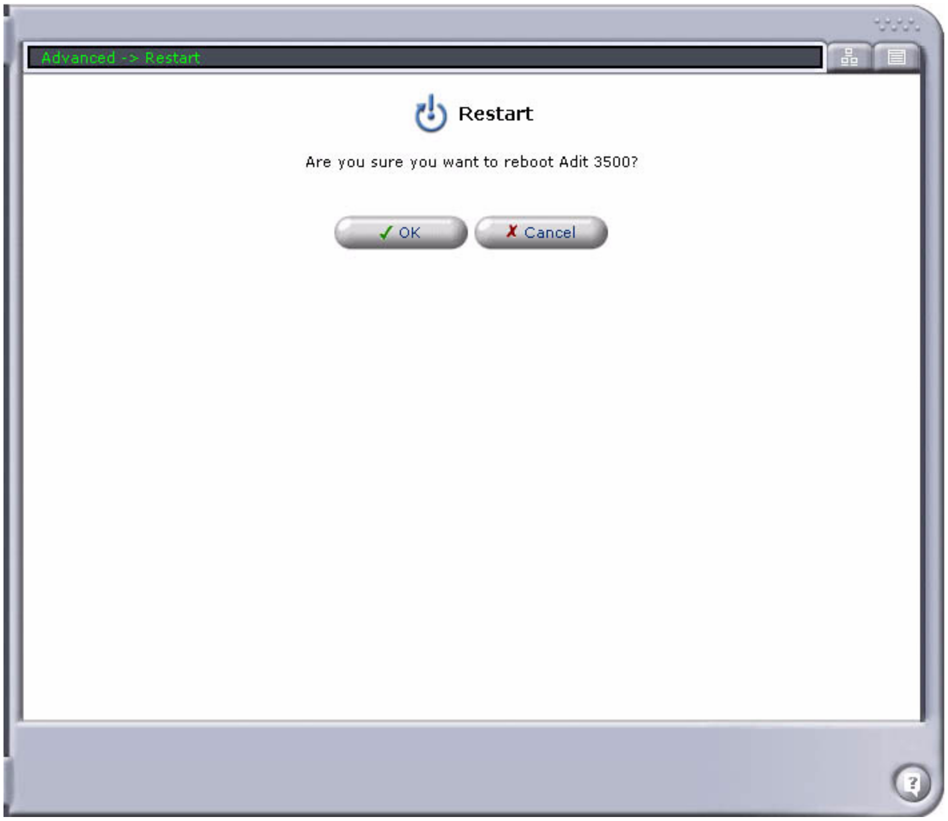
2. Select the services you wish to enable.
3. Select **OK**.

Restart

This option allows the user to reboot the Adit 3000 or MSR card.

Restarting the System

1. Select **Advanced/ Restart**.
2. Select **OK** to reboot the system.



Advanced -> Restart

Restart

Are you sure you want to reboot Adit 3500?

Restore Defaults

The Restore Defaults option sets the Adit back to its factory settings.

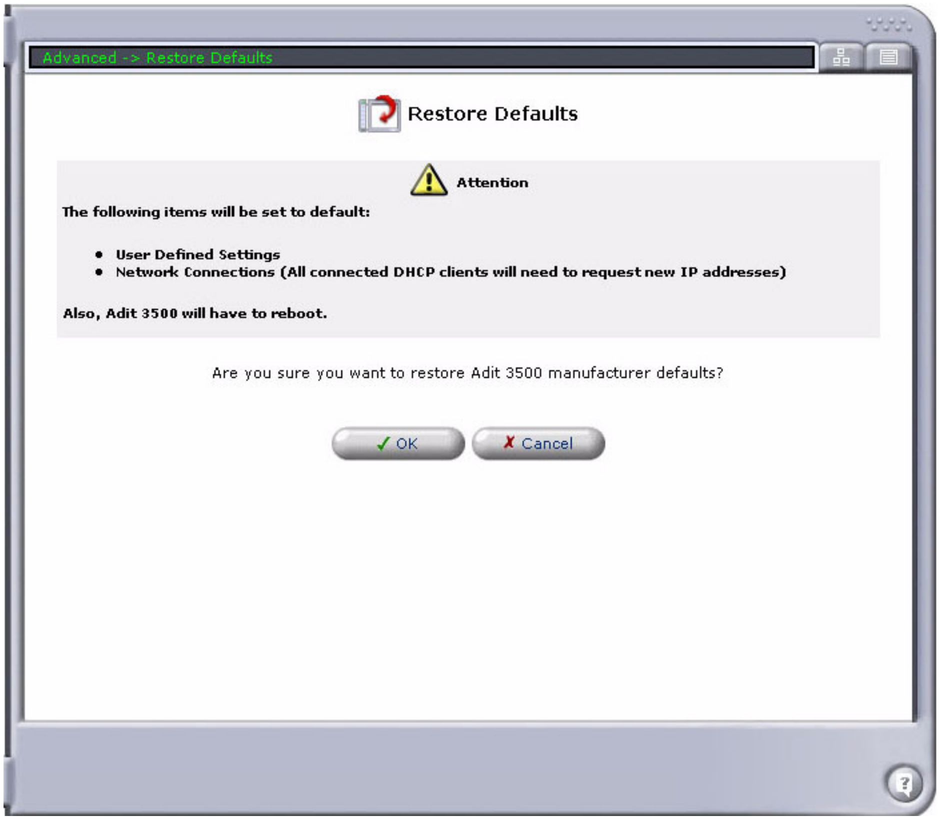
IMPORTANT: All Web-based management settings and parameters will be restored to their default values, including:

- Administrator password and all user-specified passwords
- IP address for configuration access

After the restore defaults function is complete, the Adit will reboot.

Restoring Default Settings

1. Select **Advanced/ Restore Defaults**.
2. Select **OK** to restore the defaults.



The following items will be set to default:

- User Defined Settings
- Network Connections (All connected DHCP clients will need to request new IP addresses)

Also, Adit 3500 will have to reboot.

Are you sure you want to restore Adit 3500 manufacturer defaults?

Routing

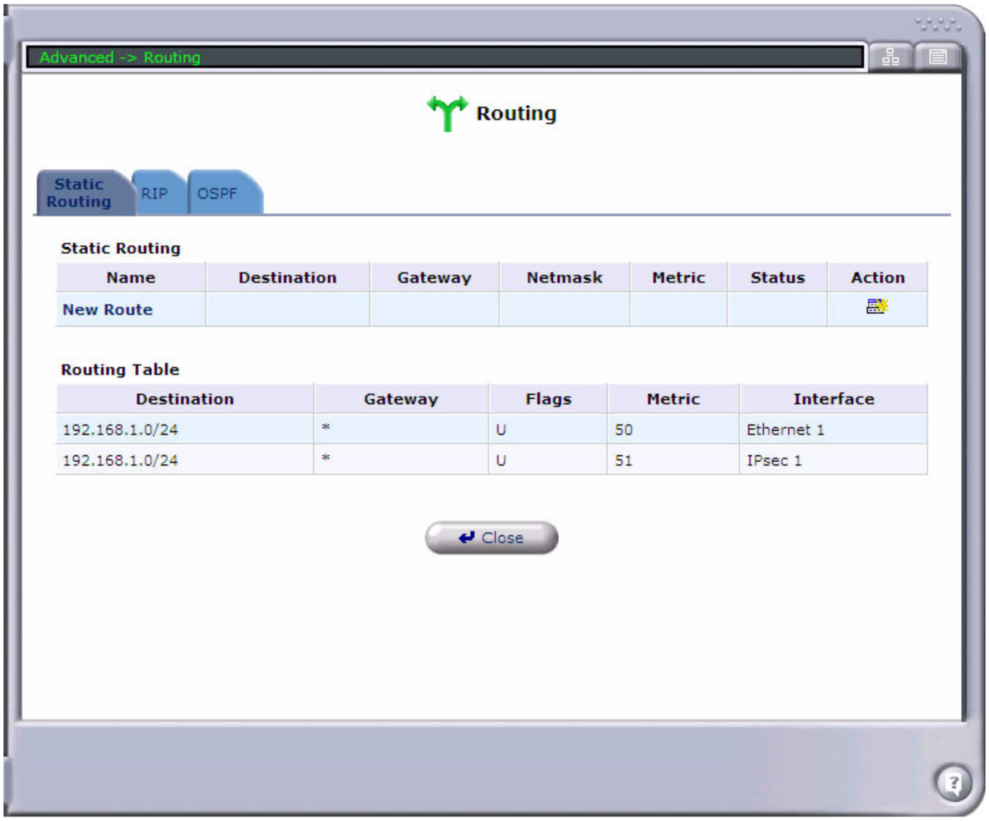
The Advanced/Routing feature provides access to configuration options for the following:

- **Static Routing**
- **RIP**
- **OSPF**

Static Routing

Select **Advanced/Routing** to view the routing table rules. This window displays the following:

- Static Routing - Displays all static routes. This table provides access to create, modify, and delete routes.
- Routing Table - Displays the current routing table.



Static Routing

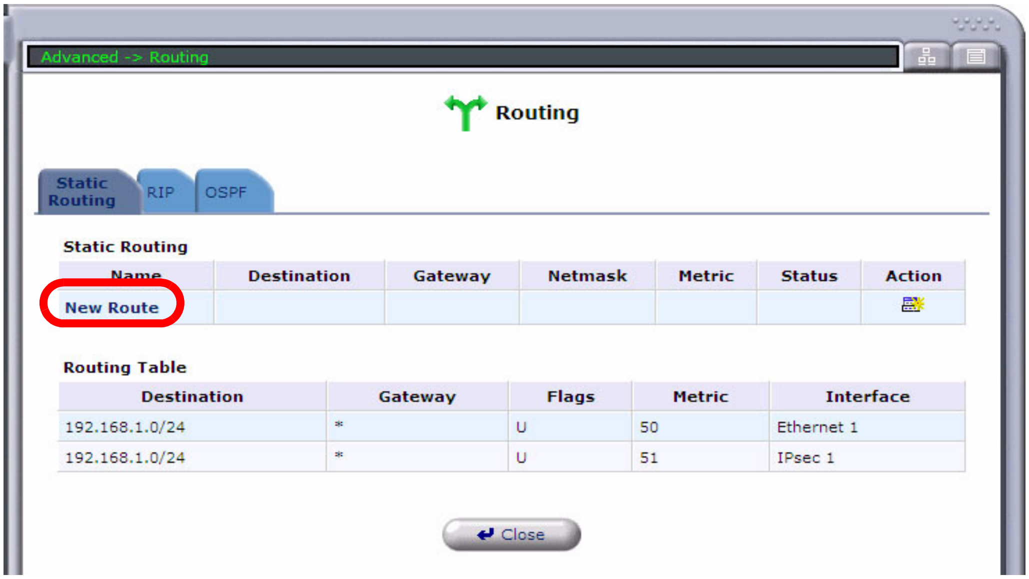
Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

Routing Table

Destination	Gateway	Flags	Metric	Interface
192.168.1.0/24	*	U	50	Ethernet 1
192.168.1.0/24	*	U	51	IPsec 1

Adding a New Route

1. Select **Advanced/ Routing**.
2. Select **New Route**.



Static Routing

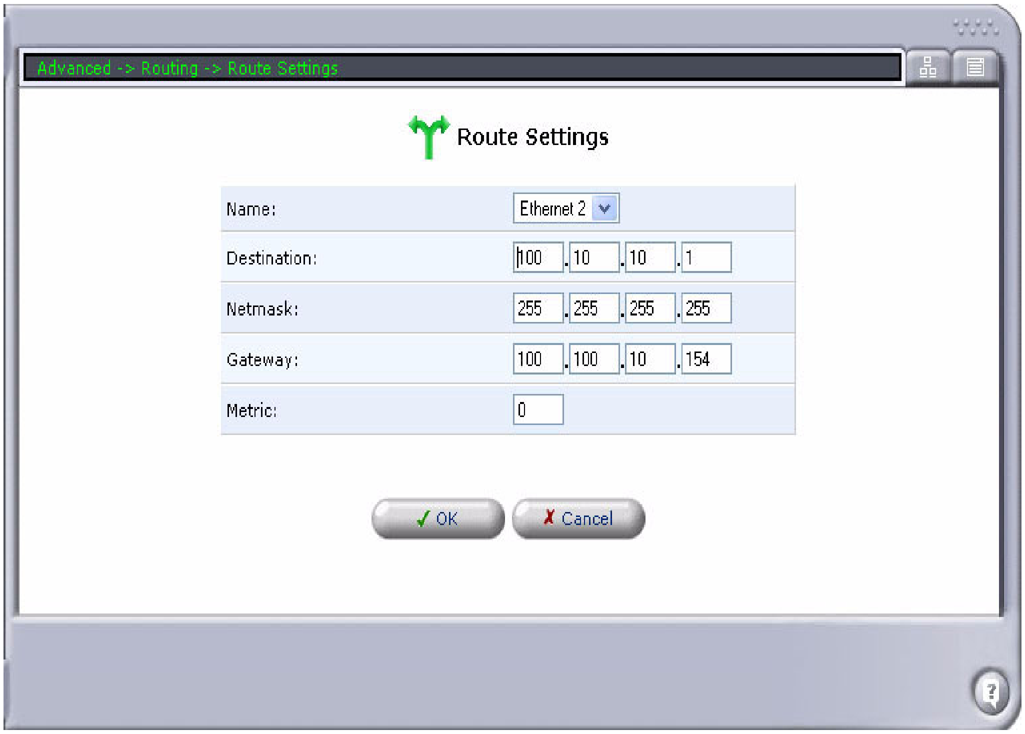
Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

Routing Table

Destination	Gateway	Flags	Metric	Interface
192.168.1.0/24	*	U	50	Ethernet 1
192.168.1.0/24	*	U	51	IPsec 1

3. Set the following fields:

Field	Definition
Name	Select a name from the Pulldown menu.
Destination	This is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0
Netmask	The Network mask is used in conjunction with the destination to determine when a route is used.
Gateway	Enter the gateway IP address.
Metric	A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.

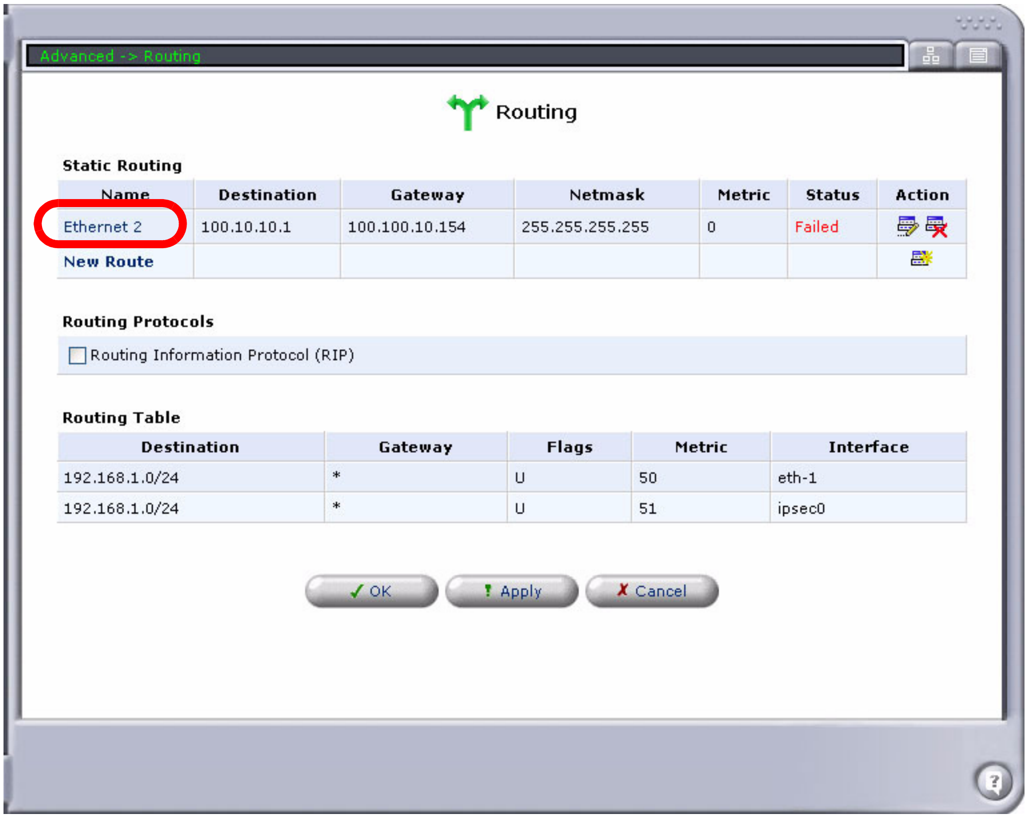


Name: Ethernet 2
Destination: 100 . 10 . 10 . 1
Netmask: 255 . 255 . 255 . 255
Gateway: 100 . 100 . 10 . 154
Metric: 0

4. Select **OK**.

Editing a Route

1. Select **Advanced/ Routing**.
2. Select a Route listed on the Routing Table (click on the name, or select the edit icon).



Routing

Static Routing

Name	Destination	Gateway	Netmask	Metric	Status	Action
Ethernet 2	100.10.10.1	100.100.10.154	255.255.255.255	0	Failed	
New Route						

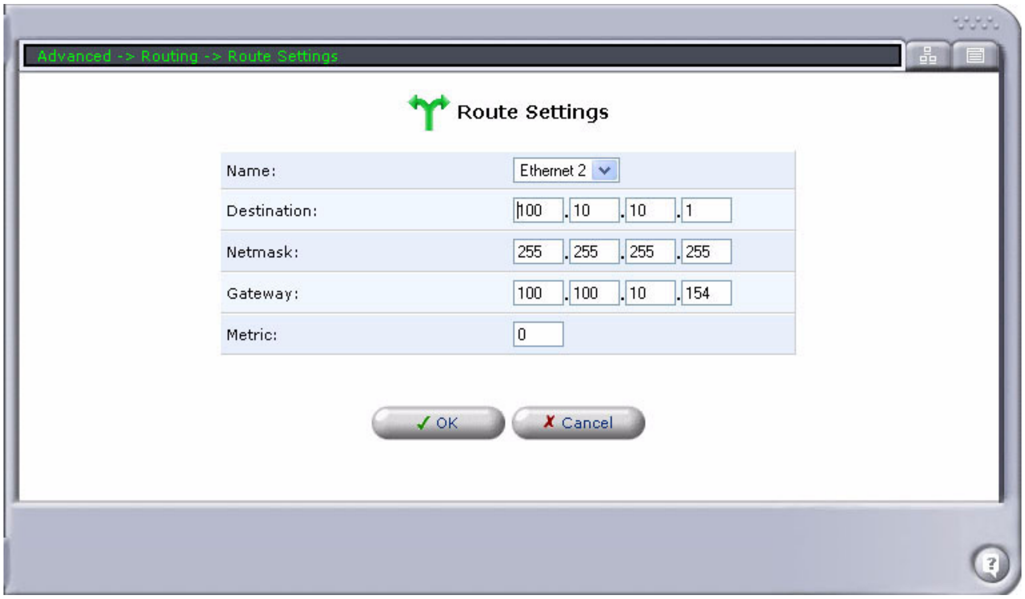
Routing Protocols

□ Routing Information Protocol (RIP)

Routing Table

Destination	Gateway	Flags	Metric	Interface
192.168.1.0/24	*	U	50	eth-1
192.168.1.0/24	*	U	51	ipsec0

3. Modify settings as needed and select **OK.**

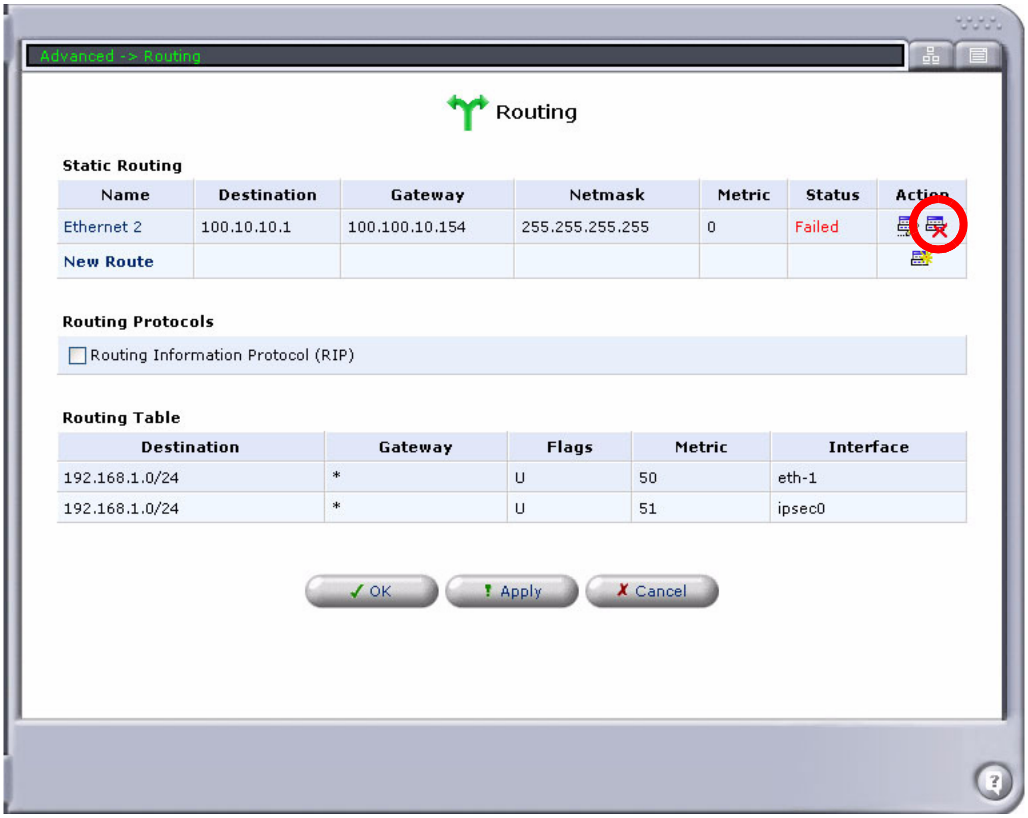


Route Settings

Name:	Ethernet 2
Destination:	100 . 10 . 10 . 1
Netmask:	255 . 255 . 255 . 255
Gateway:	100 . 100 . 10 . 154
Metric:	0

Deleting a Route

1. Select **Advanced/ Routing**.
2. Select **Action/Delete icon,** to remove the Route listed on the table.



Advanced -> Routing

Routing

Static Routing

Name	Destination	Gateway	Netmask	Metric	Status	Action
Ethernet 2	100.10.10.1	100.100.10.154	255.255.255.255	0	Failed	
New Route						

Routing Protocols

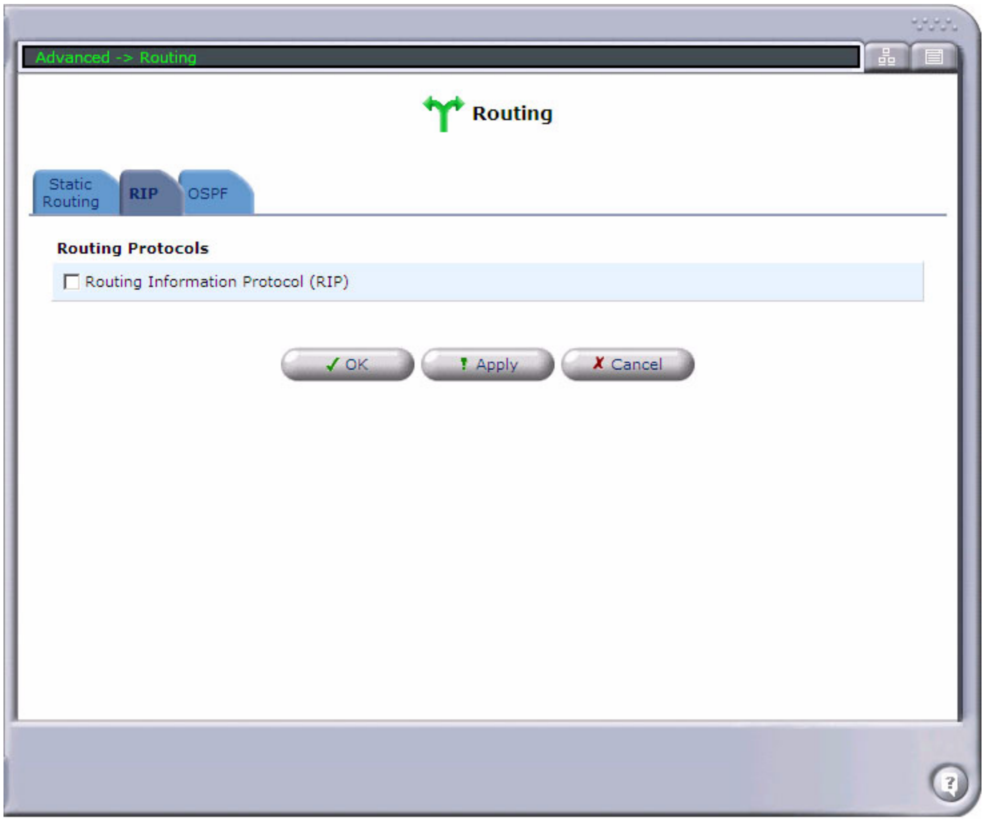
□ Routing Information Protocol (RIP)

Routing Table

Destination	Gateway	Flags	Metric	Interface
192.168.1.0/24	*	U	50	eth-1
192.168.1.0/24	*	U	51	ipsec0

RIP

Select **Advanced/Routing** and click on the **RIP** tab. The RIP window allows you to enable RIP routing.

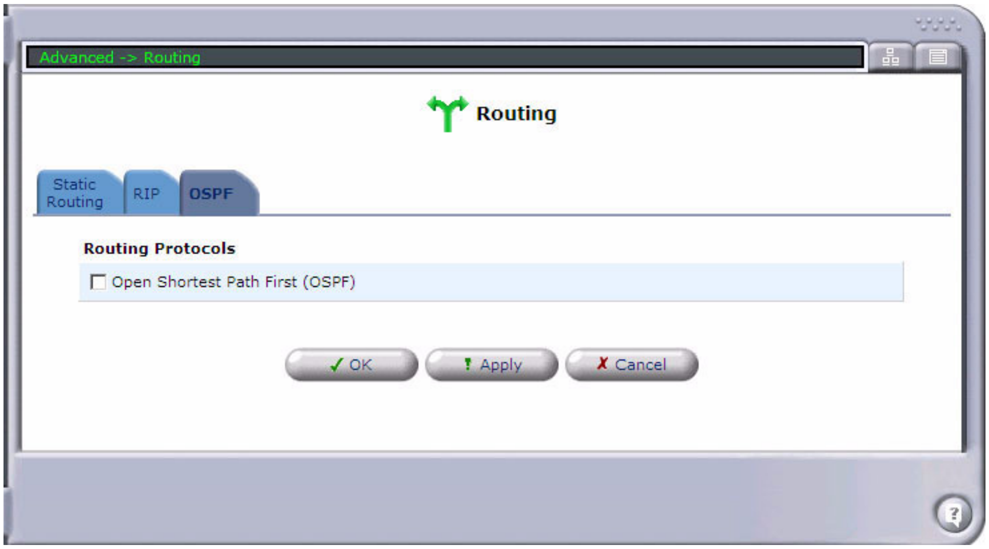


Routing Protocols

☐ Routing Information Protocol (RIP)

OSPF

Select **Advanced/Routing** and click on the **OSPF** tab. The OSPF window allows you to enable OSPF routing.

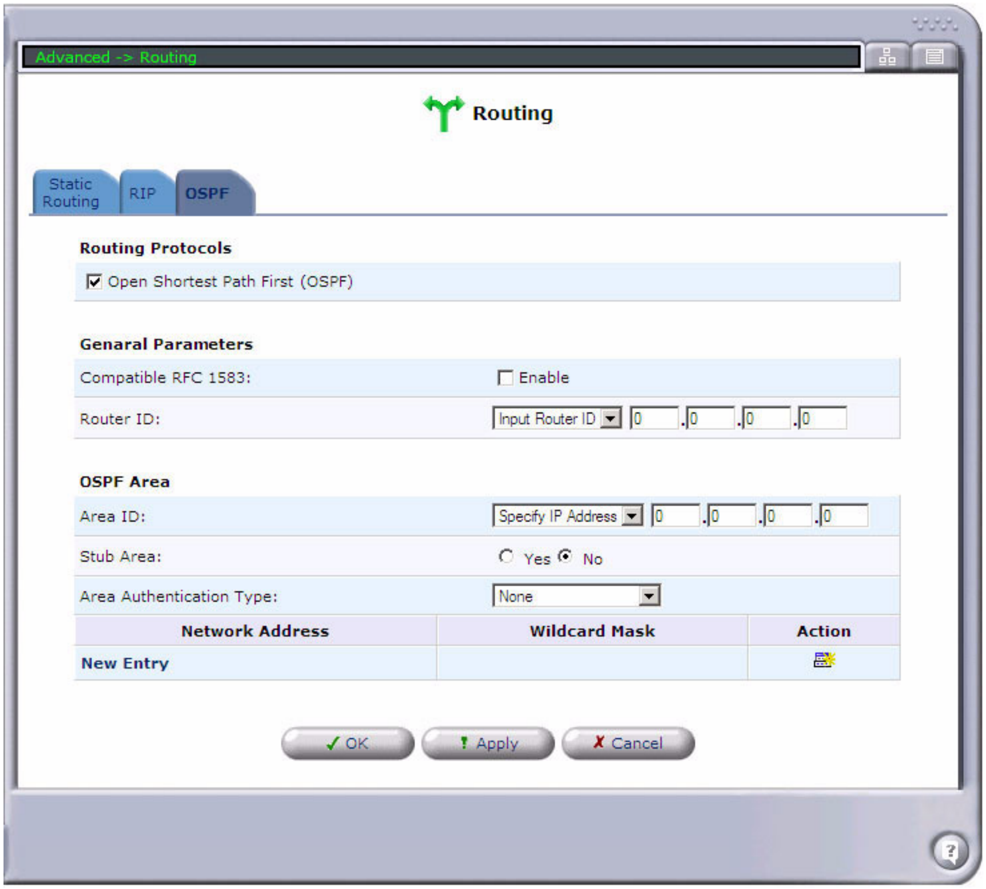


Routing Protocols

□ Open Shortest Path First (OSPF)

OSPF Field Definitions

When the Open Shortest Past First (OSPF) option is enabled, the window displays additional fields:



Routing Protocols

☑ Open Shortest Path First (OSPF)

Genaral Parameters

Compatible RFC 1583:	□ Enable
Router ID:	Input Router ID ▾ 0 .0 .0 .0

OSPF Area

Area ID:	Specify IP Address ▾ 0 .0 .0 .0
Stub Area:	○ Yes ● No
Area Authentication Type:	None ▾

Network Address	Wildcard Mask	Action
New Entry		

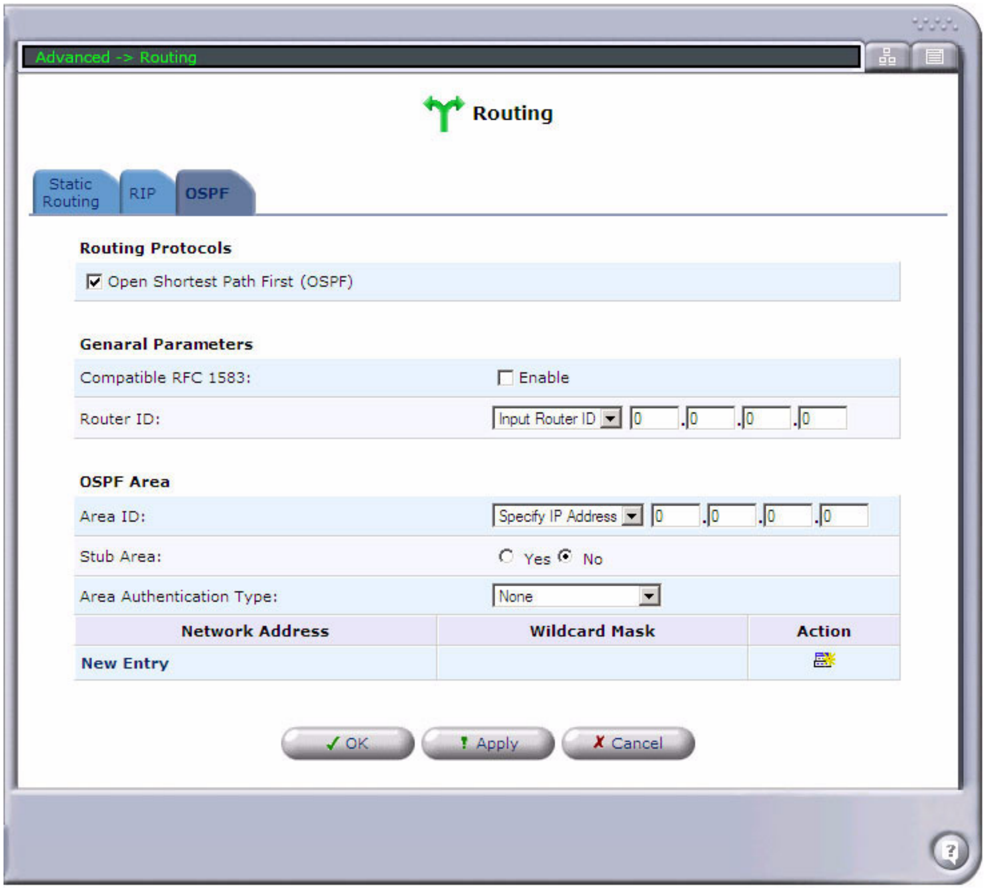
Field	Definition
Routing Protocols	
Open Shortest Path First (OSPF)	Enables OSPF.
General Parameters	Sets the OSPF Global Parameters.
Compatible RFC 1583	Enables the method used to calculate summary route costs per RFC 1583.
Router ID	**Null** - Do not use a fixed router ID. **Input Router ID** - Define a fixed router ID to be used. Enter a router IP address.
OSPF Area	Configure the OSPF Area Parameters.
Area ID	**Specify IP Address** - Enter the Area ID IP address. **Specify a Number** - Enter the Area ID number.
Stub Area	**Yes** - Define this area as a Stub area. **No** - Define this area to not be a Stub area.

Field		Definition (Continued)
	Area Authentication Type	**None** - Set the Area Authentication to none. **Simple Authentication** - Enable Simple Authentication Authentication on the OSPF Area. **Message-Digest** - Enable Message-Digest Authentication on the Area.
Network Address Table		Displays the current OSPF neighbors.
	New Entry	Select this option to open a configuration window to enter OSPF neighbors. See the following section for detailed information.

Configuring OSPF

NOTE: For interface OSPF configuration information, see *OSPF Configuration on the Network Connection* on page 3-40.

1. Select **Advanced/ Router**.
2. Select the **OSPF** tab.
3. Enable OSPF by checking the Open Shortest Path First (OSPF) checkbox.



Routing Protocols

☑ Open Shortest Path First (OSPF)

Genaral Parameters

Compatible RFC 1583:	□ Enable
Router ID:	Input Router ID 0 .0 .0 .0

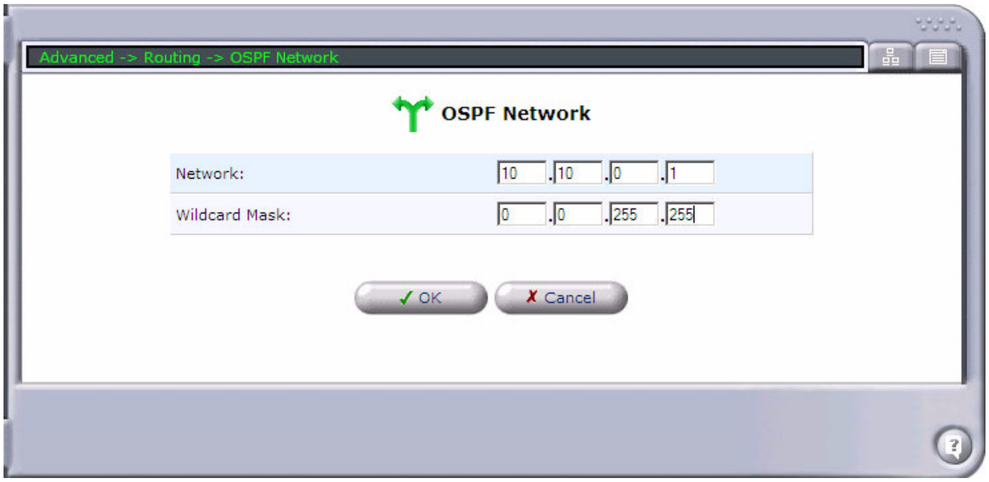
OSPF Area

Area ID:	Specify IP Address 0 .0 .0 .0
Stub Area:	○ Yes ● No
Area Authentication Type:	None

Network Address	Wildcard Mask	Action
New Entry		

4. Set Enable **Compatible RFC 1583,** if required.
5. Set **Router ID** as needed.
6. Define the **Area ID** with the Area number or Area IP Address. **Note:** 0.0.0.0 is not accepted in this field.
7. Define the Area as **Stub**, if required.
8. Define the **Area Authentication**, as required.
9. Select **New Entry**.

10. Enter the **Network** IP Address of the Neighbor to add to the OSPF Network.

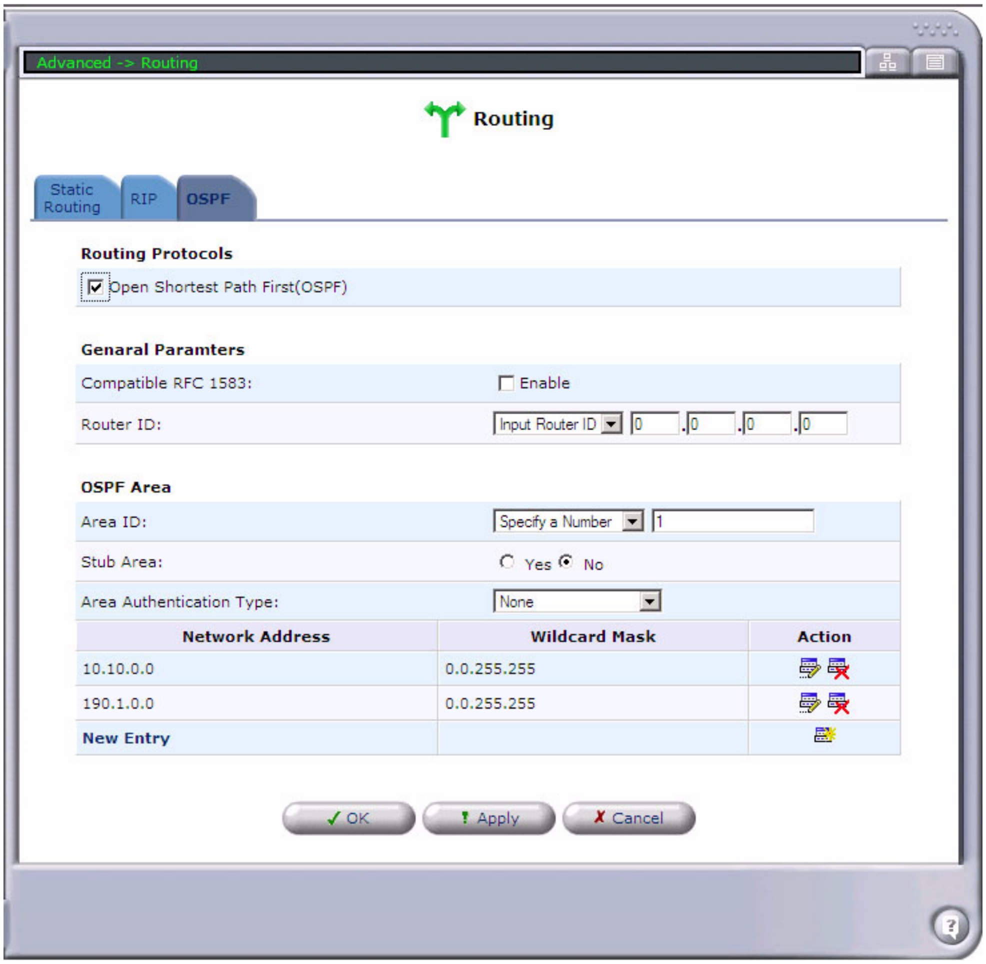


Advanced -> Routing -> OSPF Network

OSPF Network

Network:	10 . 10 . 0 . 1
Wildcard Mask:	0 . 0 . 255 . 255

11. Enter an IP address mask that includes "don’t care" bits.
12. Select **OK**. The new address appears in the Network Address Table.



Advanced -> Routing

Routing

Routing Protocols

☑ Open Shortest Path First(OSPF)

Genaral Paramters

Compatible RFC 1583:	□ Enable
Router ID:	Input Router ID ▾ 0 . 0 . 0 . 0

OSPF Area

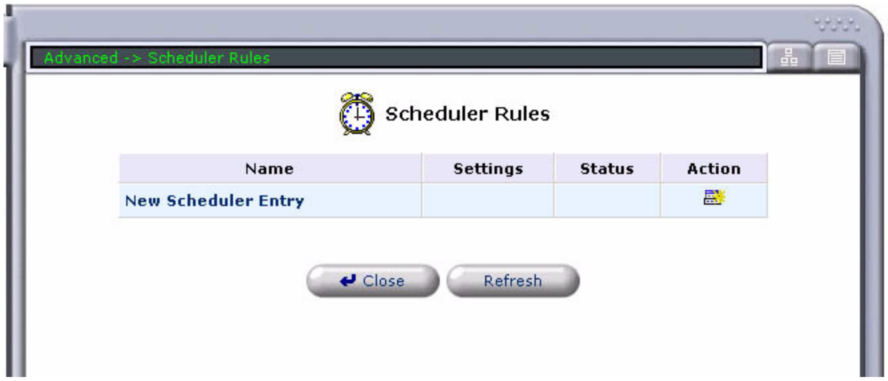
Area ID:	Specify a Number ▾ 1
Stub Area:	○ Yes ● No
Area Authentication Type:	None ▾

Network Address	Wildcard Mask	Action
10.10.0.0	0.0.255.255	
190.1.0.0	0.0.255.255	
New Entry		

Scheduler Rules

To create a scheduling rule:

1. Select **Advanced/Scheduler Rules**.

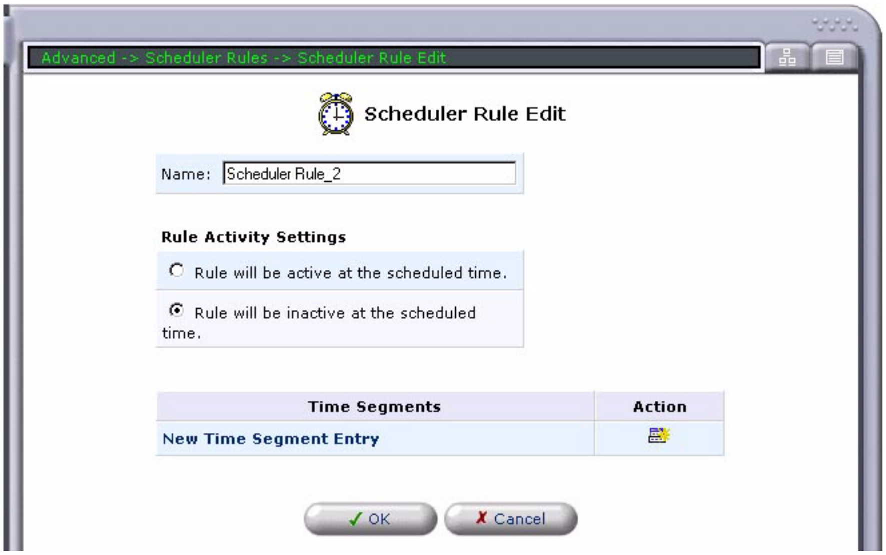


Advanced -> Scheduler Rules

Scheduler Rules

Name	Settings	Status	Action
New Scheduler Entry			

2. Select **New Scheduler Entry**.



Advanced -> Scheduler Rules -> Scheduler Rule Edit

Scheduler Rule Edit

Name: Scheduler Rule_2

Rule Activity Settings

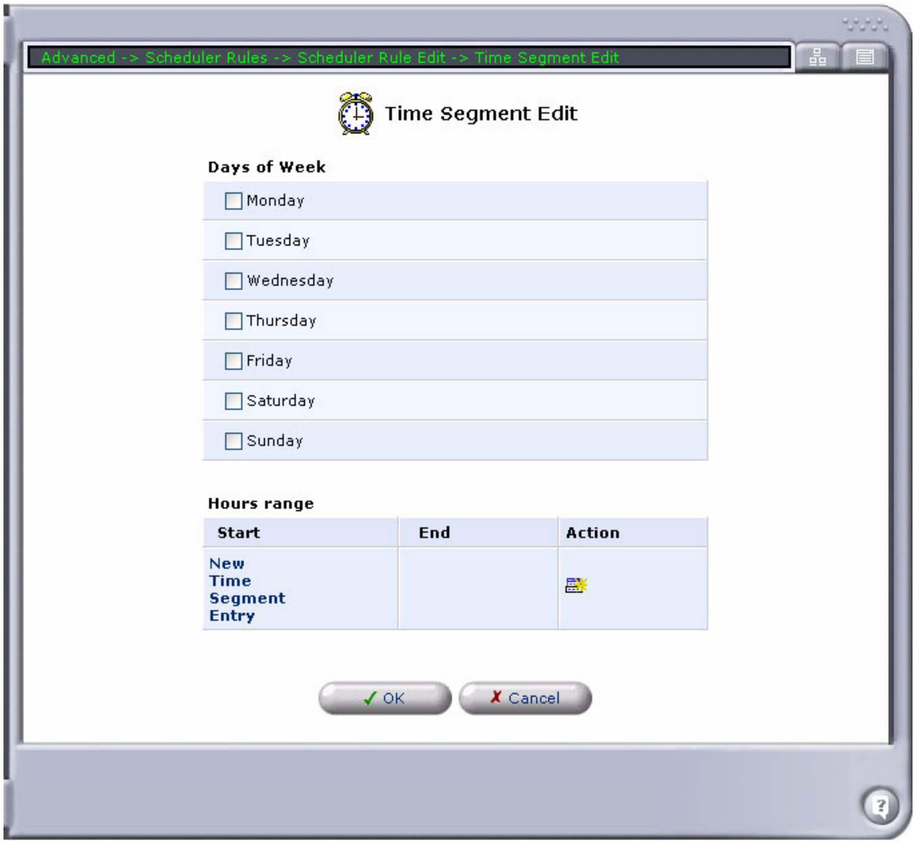
○ Rule will be active at the scheduled time.

● Rule will be inactive at the scheduled time.

Time Segments	Action
New Time Segment Entry	

3. Enter a name for the rule in the **Name** field (maximum of 64 characters).
4. Under **Rule Activity Setting,** indicate whether the rule will be active or inactive at the scheduled time.

5. Select **New Time Segment Entry** to define the day(s) of the week to apply the rule to. **Note:** At a minimum, one day must be selected.



Advanced -> Scheduler Rules -> Scheduler Rule Edit -> Time Segment Edit

Time Segment Edit

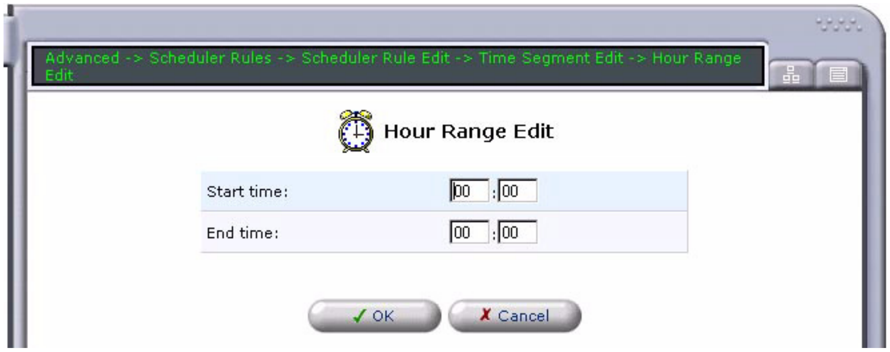
Days of Week

- □ Monday
- □ Tuesday
- □ Wednesday
- □ Thursday
- □ Friday
- □ Saturday
- □ Sunday

Hours range

Start	End	Action
New Time Segment Entry		

6. Under **Hours Range**, select **New Time Segment Entry** to define the Start and End time.

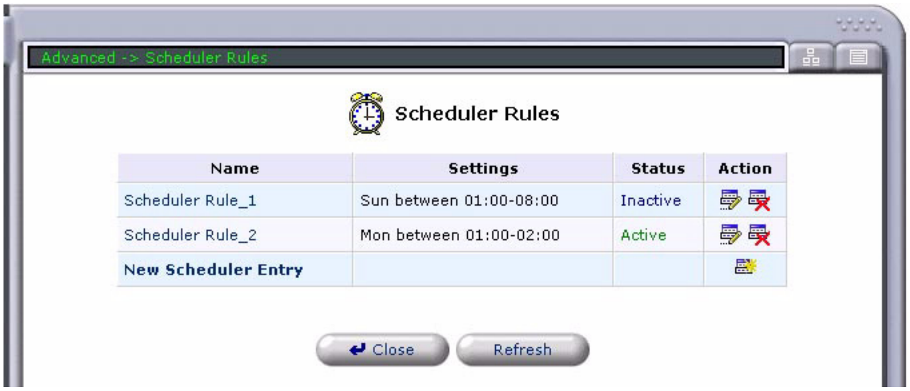


Advanced -> Scheduler Rules -> Scheduler Rule Edit -> Time Segment Edit -> Hour Range Edit

Hour Range Edit

Start time:	00 : 00
End time:	00 : 00

7. Select **OK** for each window until at the Scheduler Rules table.
   The new rule appears in the table.



Scheduler Rules

Name	Settings	Status	Action
Scheduler Rule_1	Sun between 01:00-08:00	Inactive	
Scheduler Rule_2	Mon between 01:00-02:00	Active	
New Scheduler Entry			

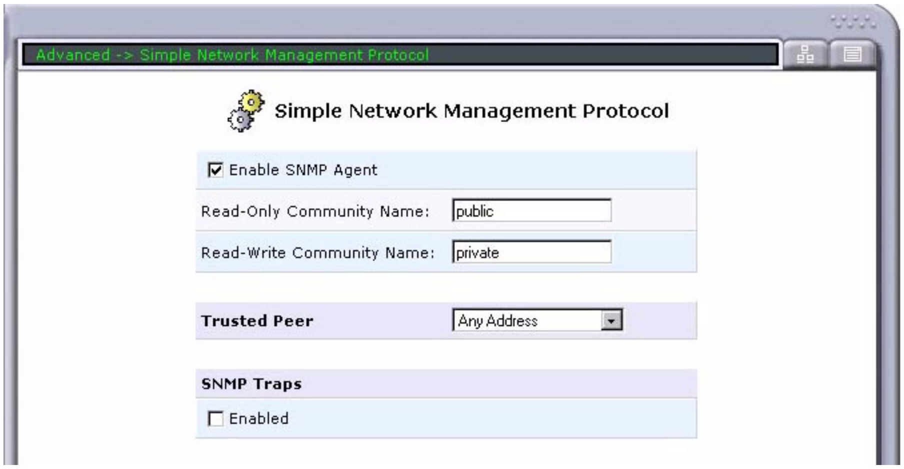
Simple Network Management Protocol

SNMP enables network management systems to remotely configure and monitor the Adit. Your Internet Service Provider (ISP) may use SNMP to identify and resolve technical problems.

Configuring the Adit's SNMP Agent

Technical information regarding the properties of the Adit's SNMP agent should be provided by your ISP. **Note:** SNMP community strings are passwords used in SNMP messages between the management system and the Adit.

1. Select **Advanced/ Simple Network Management Protocol**.


Advanced -> Simple Network Management Protocol
Simple Network Management Protocol

☑ Enable SNMP Agent

Read-Only Community Name: public

Read-Write Community Name: private

Trusted Peer: Any Address

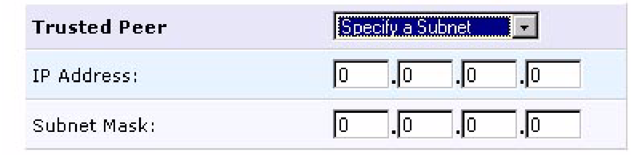
SNMP Traps

□ Enabled

2. Set the SNMP parameters, as provided by the ISP:

Field	Definition
Enable SNMP Agent	Enables the SNMP on this unit.
Read-Only Community Name	A read-only community allows the manager to monitor the Adit.
Read-Write Community Name	A read-write community allows the manager to both monitor and configure the Adit.

3. Set the **Trusted Peer**. This is the IP address and subnet that identifies which remote management stations are allowed to perform SNMP operation on the Adit.



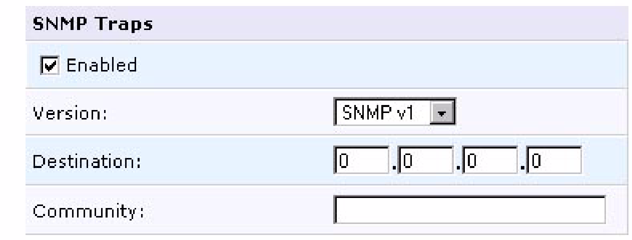
Trusted Peer: Specify a Subnet

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Field	Definition
Any Address	No restriction to remote access.
Specify an IP Address	Requires an IP address.
Specify a Subnet	Requires an IP address and Subnet.

4. Enable the **SNMP Traps**, if desired. Traps are messages sent by the Adit to a remote management station notifying the manager about important events or serious conditions. When SNMP traps are enabled, the fields expand.



SNMP Traps

☑ Enabled

Version: SNMP v1

Destination: 0 . 0 . 0 . 0

Community:

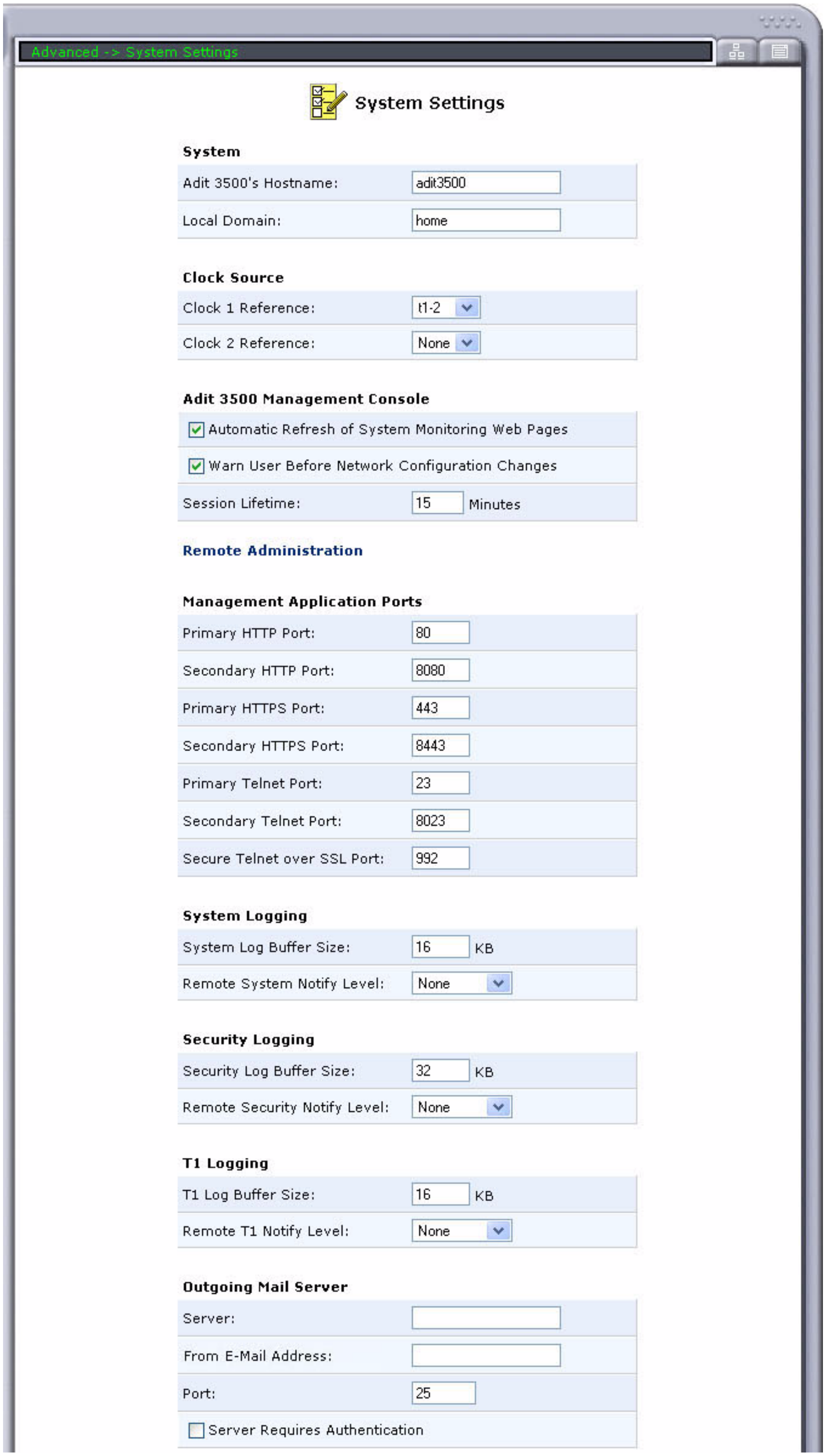
Field	Definition
Enable	Check to enable the SNMP traps.
Version	SNMP v1- SNMP version 1 SNMP v2c - SNMP version 2C
Destination	Enter the Destination IP address.
Community	Enter a community string (a password that allows access to a network device).

System Settings

Select **Advanced/System Settings** to view and modify general system settings.

As shown in the screen shots on the following pages, the system settings differ slightly between the Adit 3000 and MSR. For example, the MSR does not support the Clock Source fields, and T1 Logging is replaced by LCC (Link Cross-Connect) Logging.

Adit 3500



Advanced -> System Settings

System Settings

System

Adit 3500's Hostname:	adit3500
Local Domain:	home

Clock Source

Clock 1 Reference:	t1-2
Clock 2 Reference:	None

Adit 3500 Management Console

☑ Automatic Refresh of System Monitoring Web Pages

☑ Warn User Before Network Configuration Changes

Session Lifetime:	15 Minutes

Remote Administration

Management Application Ports

Primary HTTP Port:	80
Secondary HTTP Port:	8080
Primary HTTPS Port:	443
Secondary HTTPS Port:	8443
Primary Telnet Port:	23
Secondary Telnet Port:	8023
Secure Telnet over SSL Port:	992

System Logging

System Log Buffer Size:	16 KB
Remote System Notify Level:	None

Security Logging

Security Log Buffer Size:	32 KB
Remote Security Notify Level:	None

T1 Logging

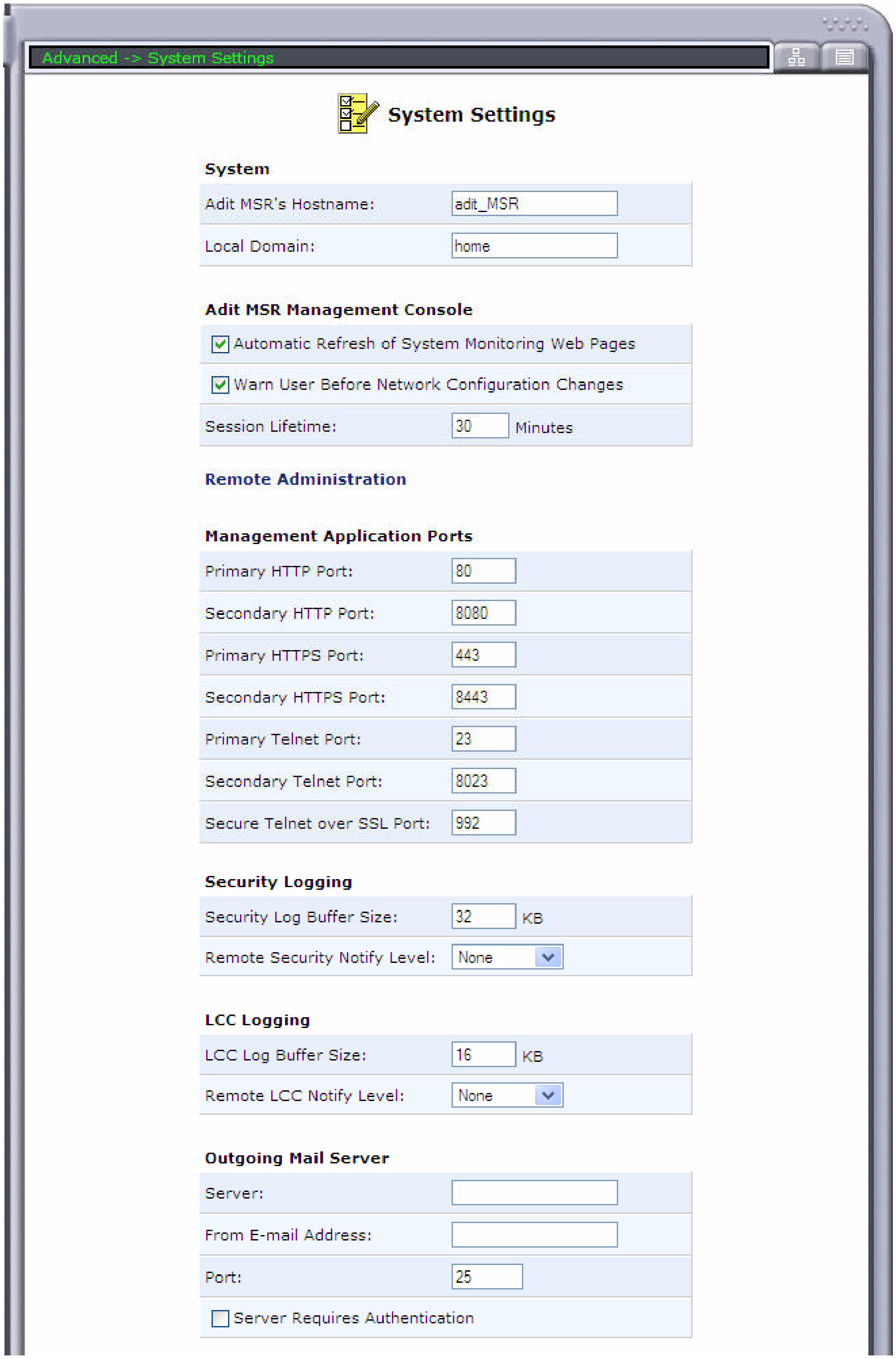
T1 Log Buffer Size:	16 KB
Remote T1 Notify Level:	None

Outgoing Mail Server

Server:	
From E-Mail Address:	
Port:	25

☐ Server Requires Authentication

Adit MSR



Advanced -> System Settings

System Settings

System

Adit MSR's Hostname:	adit_MSR
Local Domain:	home

Adit MSR Management Console

☑ Automatic Refresh of System Monitoring Web Pages

☑ Warn User Before Network Configuration Changes

Session Lifetime:	30 Minutes

Remote Administration

Management Application Ports

Primary HTTP Port:	80
Secondary HTTP Port:	8080
Primary HTTPS Port:	443
Secondary HTTPS Port:	8443
Primary Telnet Port:	23
Secondary Telnet Port:	8023
Secure Telnet over SSL Port:	992

Security Logging

Security Log Buffer Size:	32 KB
Remote Security Notify Level:	None

LCC Logging

LCC Log Buffer Size:	16 KB
Remote LCC Notify Level:	None

Outgoing Mail Server

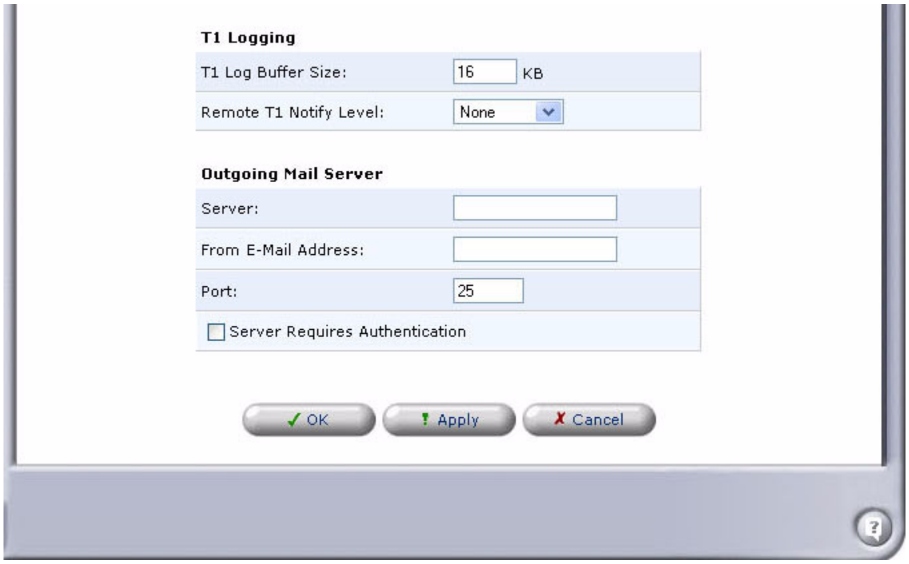
Server:	
From E-mail Address:	
Port:	25

□ Server Requires Authentication

Defining an Outgoing Mail Server

Features that require the Adit to send e-mail (example: e-mail notification) require an outgoing SMTP server to be defined.

1. Enter the host name of your outgoing SMTP server in the **Server** field.
2. Enter a "from" e-mail address in the **From E-mail Address field**.
   Each e-mail requires a "from" address. Some outgoing servers refuse to forward e-mail without a valid "from" address for anti-spam considerations.



T1 Logging

T1 Log Buffer Size:	16 KB
Remote T1 Notify Level:	None

Outgoing Mail Server

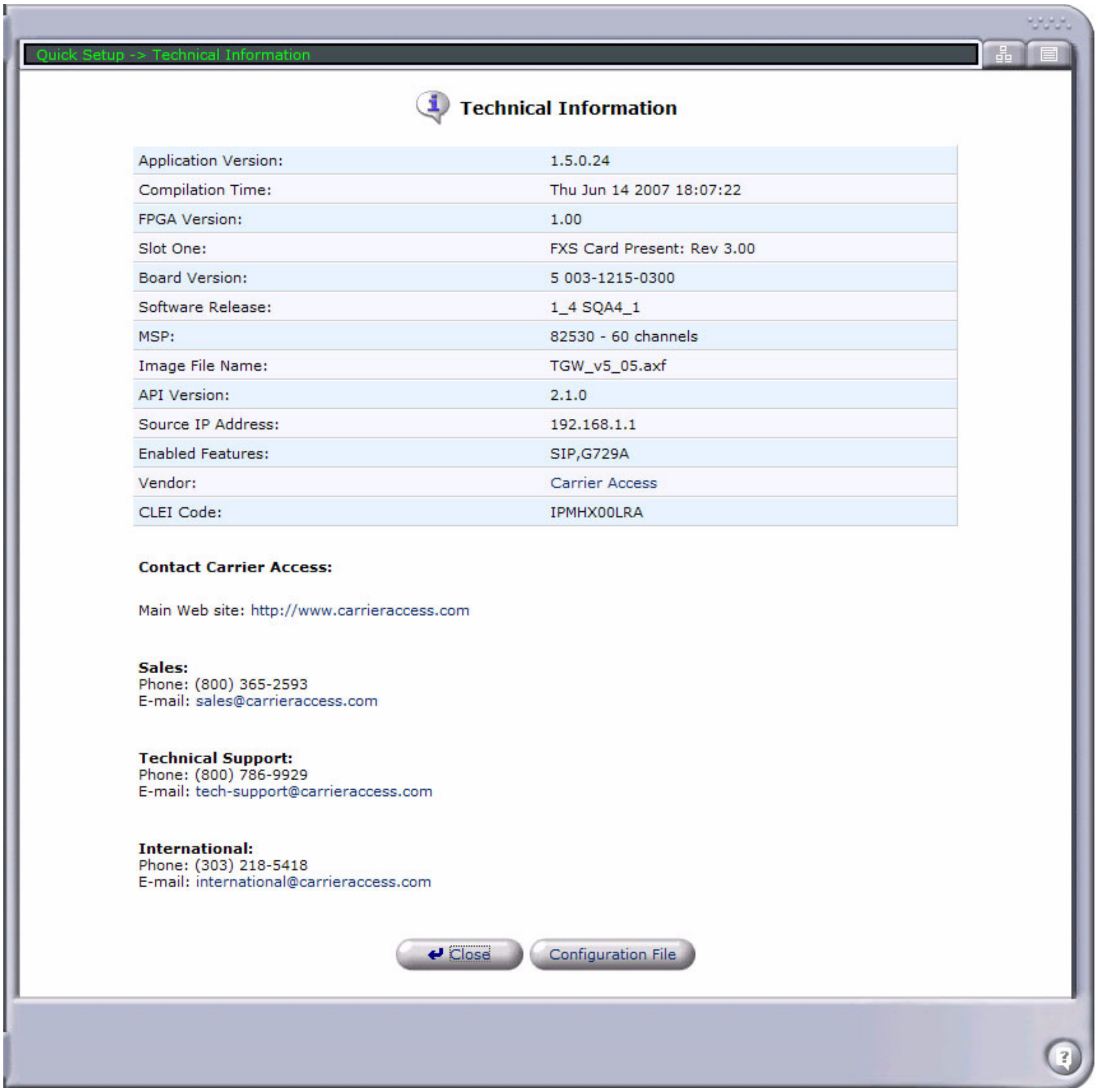
Server:	
From E-Mail Address:	
Port:	25
□ Server Requires Authentication	

Technical Information

Select **Advanced/Technical Information** to view technical information about the system, including software version numbers and contact information.

As shown in the following screen shots, the technical information differs slightly between the Adit 3000 and MSR. For example, the MSR technical information includes the boot version, memory size, and slot position in the Adit 600 chassis.

Adit 3500



Technical Information

Application Version:	1.5.0.24
Compilation Time:	Thu Jun 14 2007 18:07:22
FPGA Version:	1.00
Slot One:	FXS Card Present: Rev 3.00
Board Version:	5 003-1215-0300
Software Release:	1_4 SQA4_1
MSP:	82530 - 60 channels
Image File Name:	TGW_v5_05.axf
API Version:	2.1.0
Source IP Address:	192.168.1.1
Enabled Features:	SIP,G729A
Vendor:	Carrier Access
CLEI Code:	IPMHX00LRA

Contact Carrier Access:

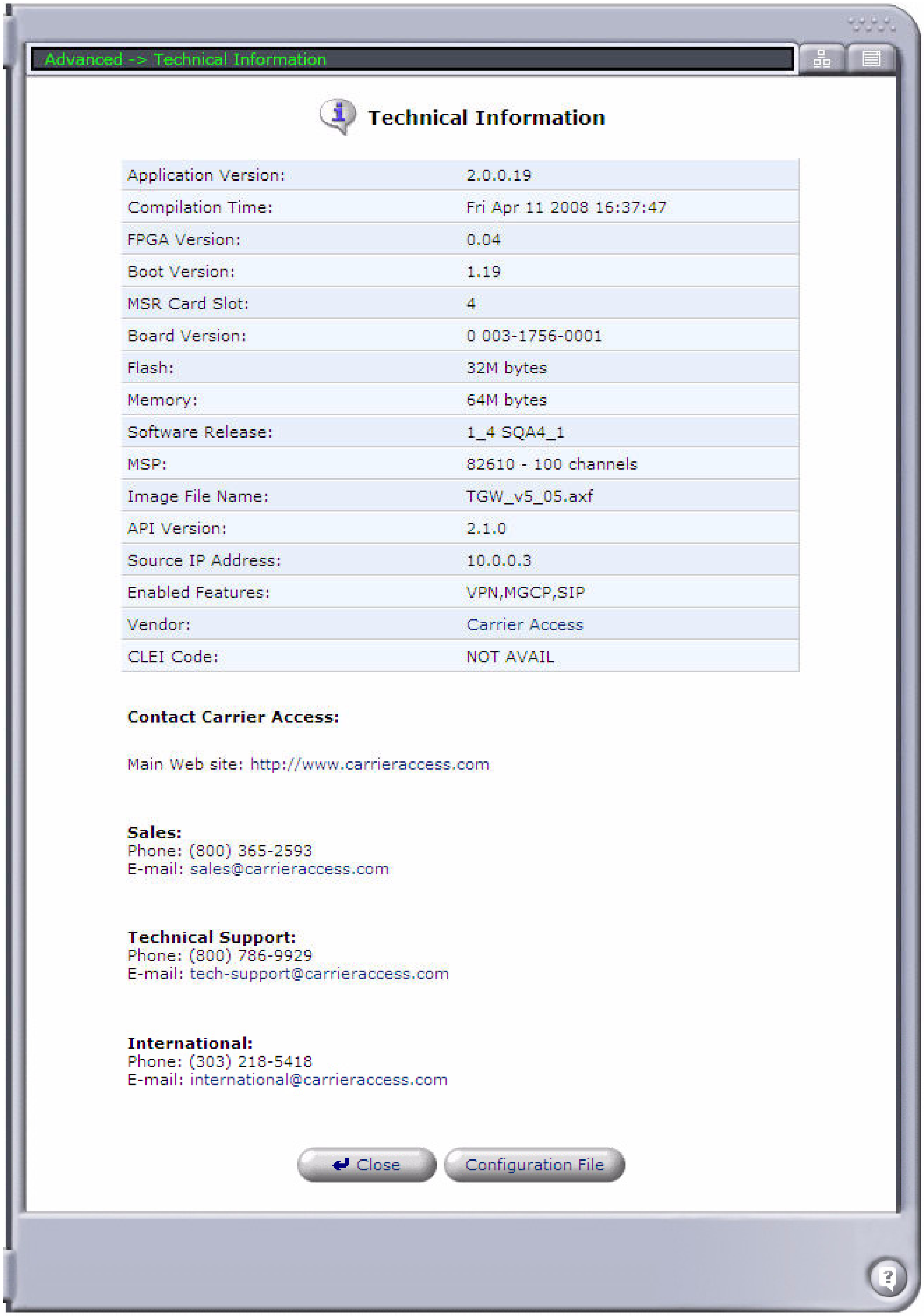
Main Web site: http://www.carrieraccess.com

Sales:
Phone: (800) 365-2593
E-mail: sales@carrieraccess.com

Technical Support:
Phone: (800) 786-9929
E-mail: tech-support@carrieraccess.com

International:
Phone: (303) 218-5418
E-mail: international@carrieraccess.com

Adit MSR



Technical Information

Application Version:	2.0.0.19
Compilation Time:	Fri Apr 11 2008 16:37:47
FPGA Version:	0.04
Boot Version:	1.19
MSR Card Slot:	4
Board Version:	0 003-1756-0001
Flash:	32M bytes
Memory:	64M bytes
Software Release:	1_4 SQA4_1
MSP:	82610 - 100 channels
Image File Name:	TGW_v5_05.axf
API Version:	2.1.0
Source IP Address:	10.0.0.3
Enabled Features:	VPN,MGCP,SIP
Vendor:	Carrier Access
CLEI Code:	NOT AVAIL

Contact Carrier Access:

Main Web site: http://www.carrieraccess.com

Sales:
Phone: (800) 365-2593
E-mail: sales@carrieraccess.com

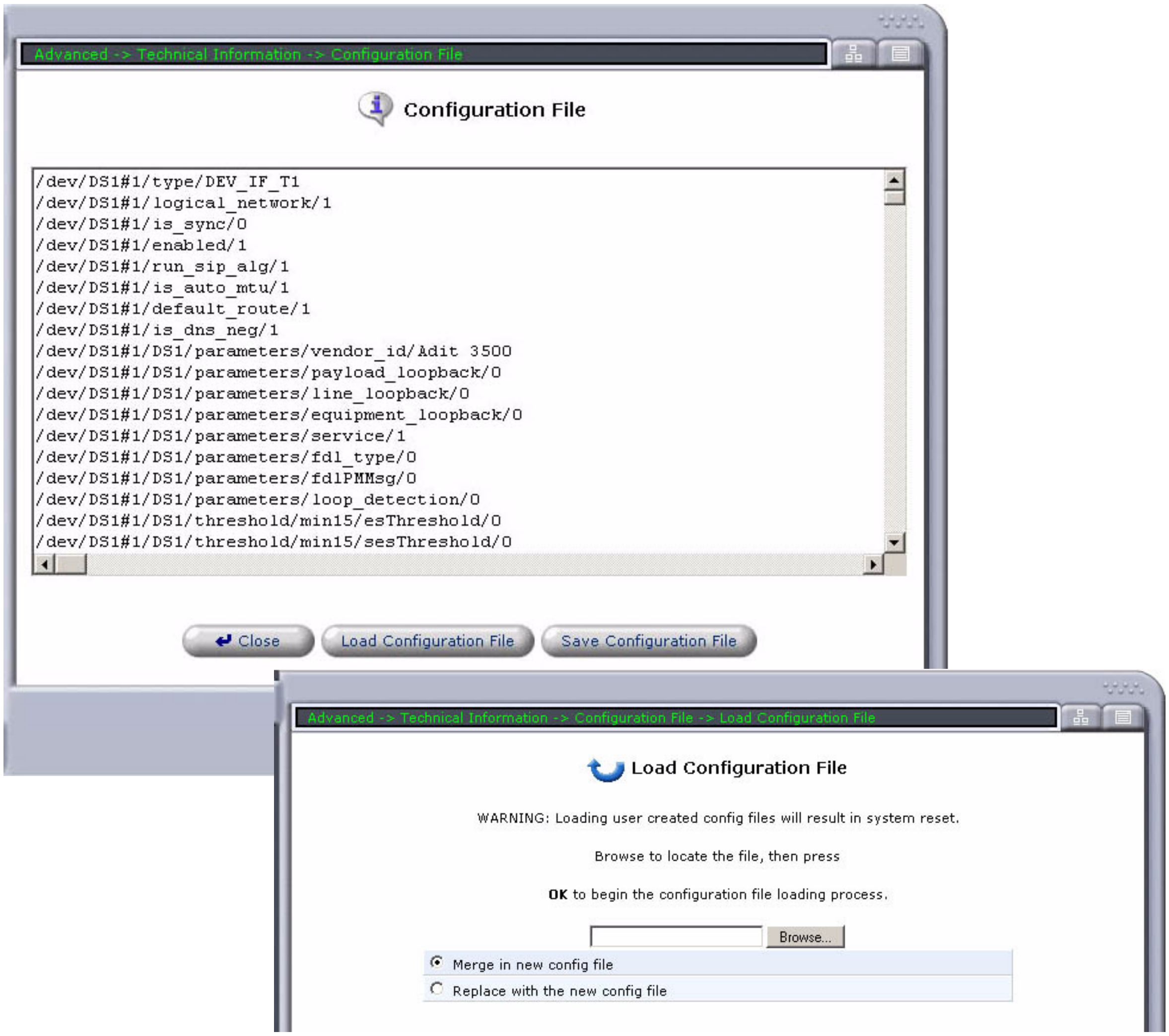
Technical Support:
Phone: (800) 786-9929
E-mail: tech-support@carrieraccess.com

International:
Phone: (303) 218-5418
E-mail: international@carrieraccess.com

Configuration File

The Configuration File button on the Technical Information window displays the current configuration file for the system. The configuration file can be saved, modified, and reloaded, if necessary.

This feature can simplify the process of modifying one or more variables of a configuration and loading it onto the original or other Adits.


Advanced -> Technical Information -> Configuration File
Configuration File
Close
Load Configuration File
Save Configuration File
Advanced -> Technical Information -> Configuration File -> Load Configuration File
Load Configuration File
Browse...

```
/dev/DS1#1/type/DEV_IF_T1
/dev/DS1#1/logical_network/1
/dev/DS1#1/is_sync/0
/dev/DS1#1/enabled/1
/dev/DS1#1/run_sip_alg/1
/dev/DS1#1/is_auto_mtu/1
/dev/DS1#1/default_route/1
/dev/DS1#1/is_dns_neg/1
/dev/DS1#1/DS1/parameters/vendor_id/Adit 3500
/dev/DS1#1/DS1/parameters/payload_loopback/0
/dev/DS1#1/DS1/parameters/line_loopback/0
/dev/DS1#1/DS1/parameters/equipment_loopback/0
/dev/DS1#1/DS1/parameters/service/1
/dev/DS1#1/DS1/parameters/fdl_type/0
/dev/DS1#1/DS1/parameters/fdlPMMsg/0
/dev/DS1#1/DS1/parameters/loop_detection/0
/dev/DS1#1/DS1/threshold/min15/esThreshold/0
/dev/DS1#1/DS1/threshold/min15/sesThreshold/0
```

WARNING: Loading user created config files will result in system reset.

Browse to locate the file, then press

OK to begin the configuration file loading process.

● Merge in new config file

○ Replace with the new config file

WARNING! ALL PASSWORDS ON THE SYSTEM WILL BE RESET TO DEFAULT VALUES WHEN THE "REPLACE WITH THE NEW CONFIG FILE" OPTION IS SELECTED.

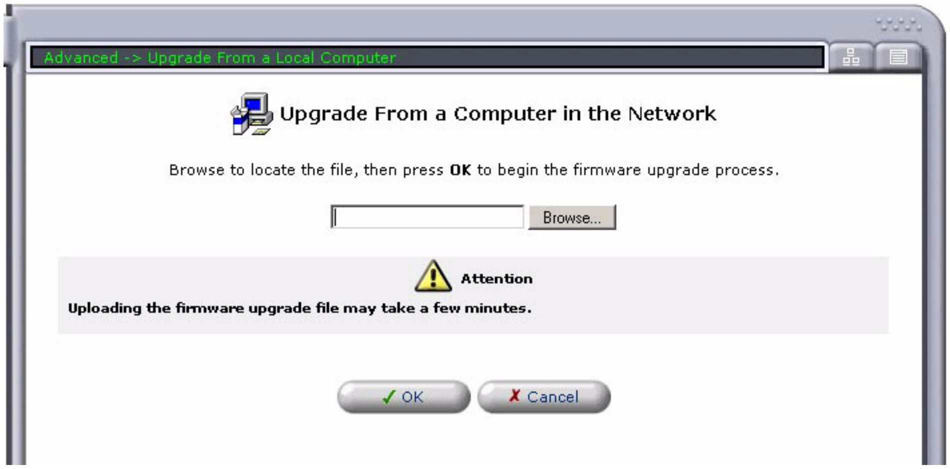
Field	Definition
Save Configuration File	The system walks you through the saving of the configuration.
Load Configuration File	The system opens a new window and asks you to locate a configuration file. Once located, you have the following options: **Merge in new config file** - modify the configuration. **Replace with the new config file** - replace the configuration.

Upgrade From a Local Computer

This feature allows the user to easily upgrade the Adit software.

Upgrading the Software

1. Select **Advanced/ Upgrade From a Local Computer**.



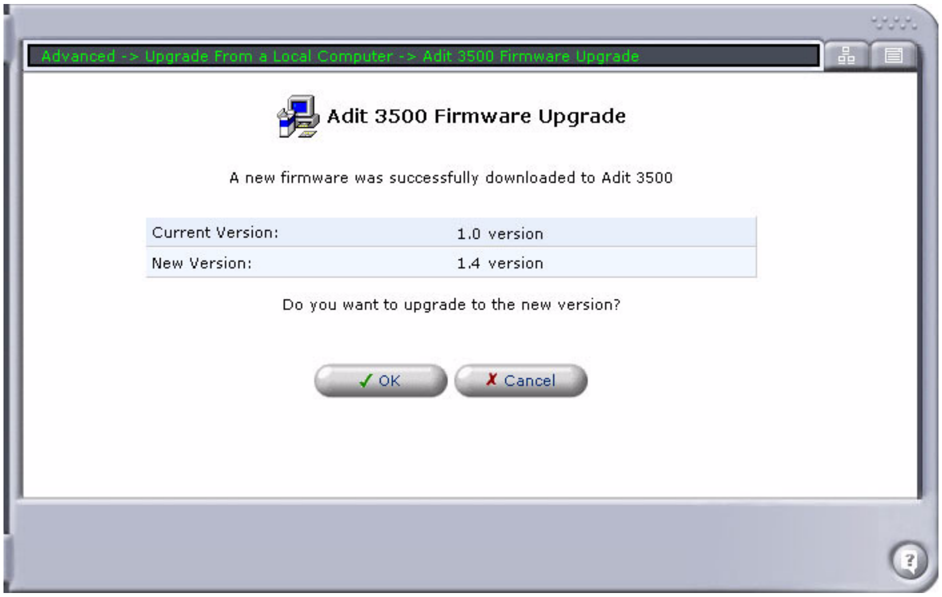
Upgrade From a Computer in the Network

Browse to locate the file, then press **OK** to begin the firmware upgrade process.

Attention

Uploading the firmware upgrade file may take a few minutes.

2. Select the **Browse** button and select the upgrade file (example: adit3000_1_6.rmt).
3. Select **OK** to download the file.



Advanced -> Upgrade From a Local Computer -> Adit 3500 Firmware Upgrade

Adit 3500 Firmware Upgrade

A new firmware was successfully downloaded to Adit 3500

Current Version:	1.0 version
New Version:	1.4 version

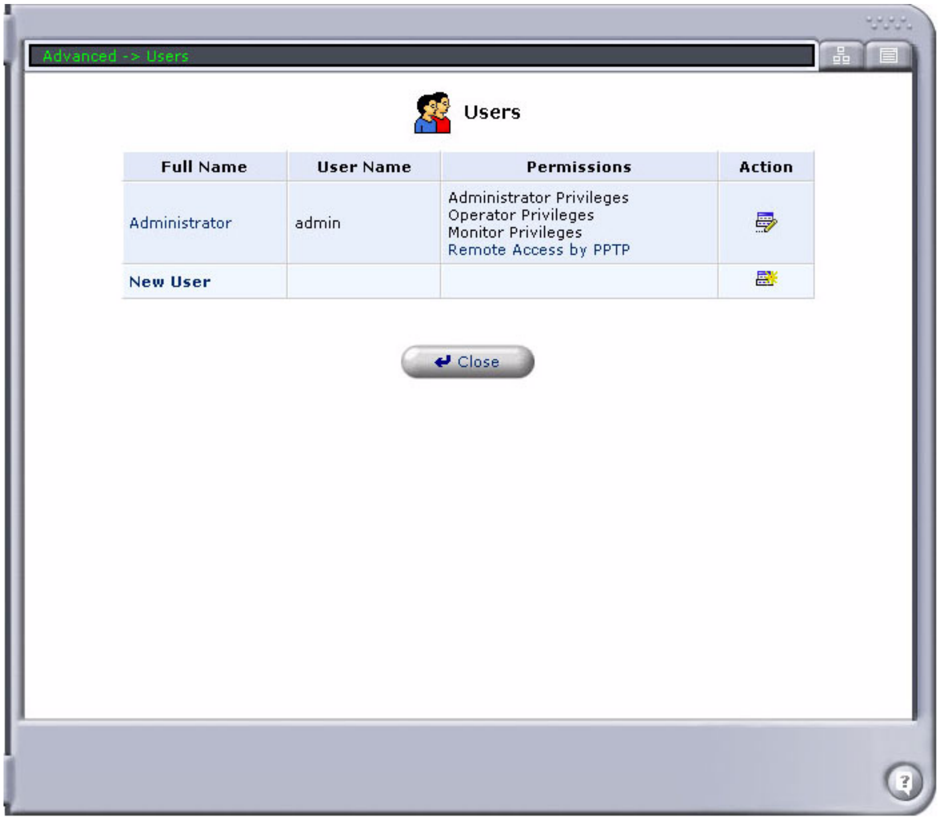
Do you want to upgrade to the new version?

4. If the download was successful, select **OK** to upgrade the system.

Users

Use this feature to view, add, edit, and delete users on the device, and to configure e-mail notification.

NOTE: Do not add more that 25 users to the system.



Advanced -> Users

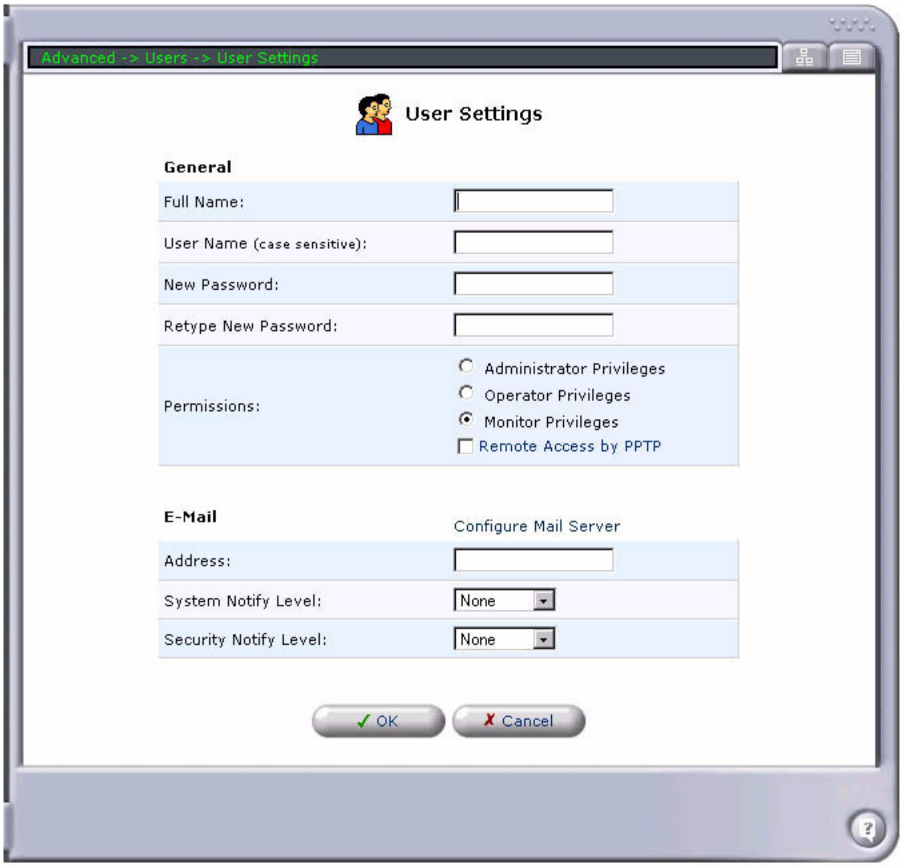
Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Privileges Operator Privileges Monitor Privileges Remote Access by PPTP	
New User			

Adding a User

1. Select **Advanced/ Users**.
2. Select **New User** and enter the following General information:

Field	Definition
General	
Full Name	The user's full name.
User Name	The name this user will enter (as user name) to access this network.
New Password	The password for this user.
Retype New Password	Retype password to confirm.
Permissions	**Administrator Privileges** - Full access to system. **Operator Privileges** - Access to all but user management. **Monitor Privileges** - Read-only access. **Remote Access by PPTP** - see **Advanced/*PPTP (Point-to-Point Tunneling Protocol)***



Advanced -> Users -> User Settings

User Settings

General

Full Name:	
User Name (case sensitive):	
New Password:	
Retype New Password:	
Permissions:	○ Administrator Privileges ○ Operator Privileges ● Monitor Privileges □ Remote Access by PPTP

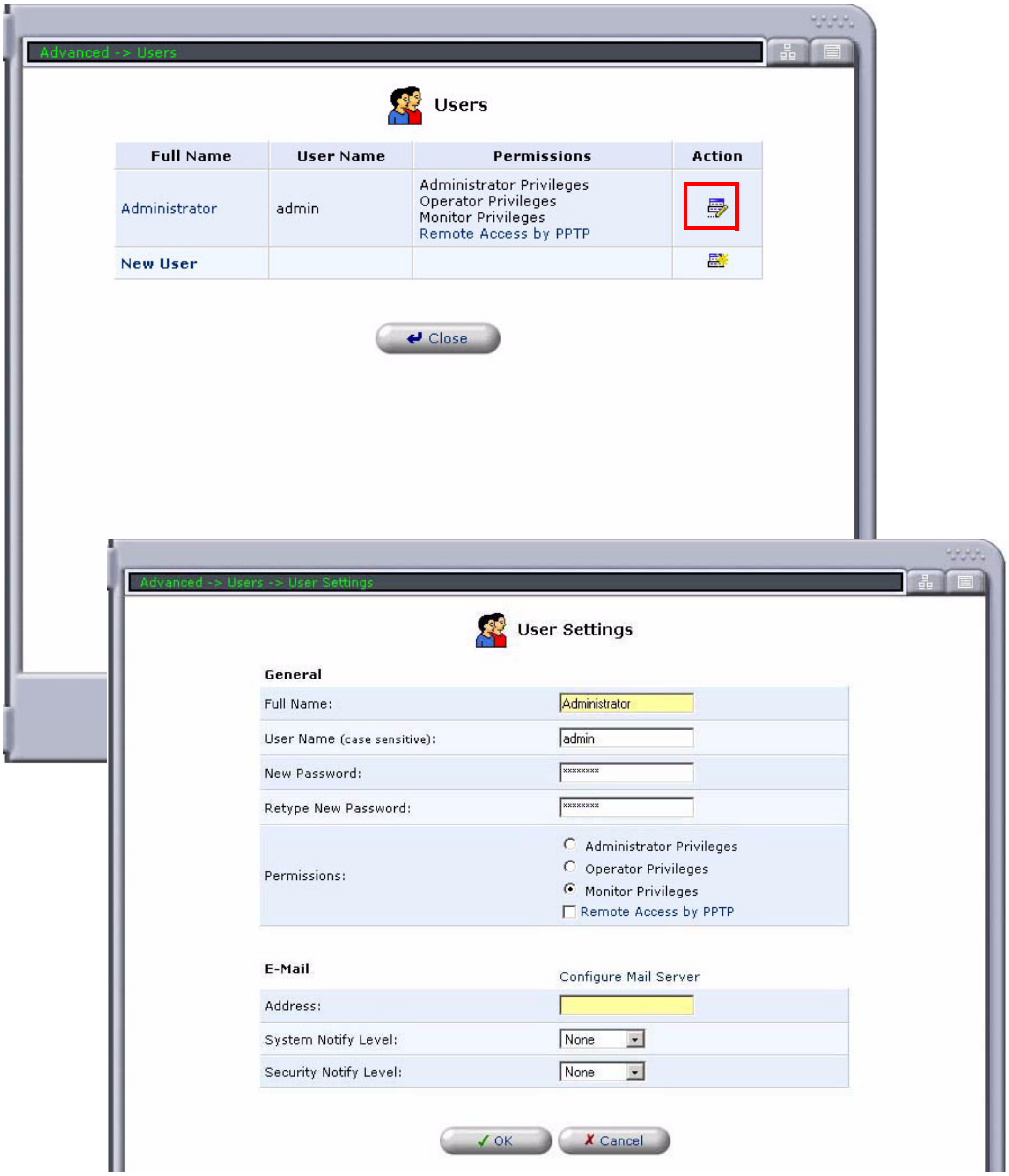
E-Mail Configure Mail Server

Address:	
System Notify Level:	None
Security Notify Level:	None

3. Select **OK**.

Editing a User

1. Select **Advanced/ Users**.
2. Select the **Action/Edit** icon of an existing User.
3. Modify fields as needed.



Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Privileges Operator Privileges Monitor Privileges Remote Access by PPTP	
New User			

User Settings

General

Full Name:	Administrator
User Name (case sensitive):	admin
New Password:	********
Retype New Password:	********
Permissions:	○ Administrator Privileges ○ Operator Privileges ● Monitor Privileges □ Remote Access by PPTP

E-Mail Configure Mail Server

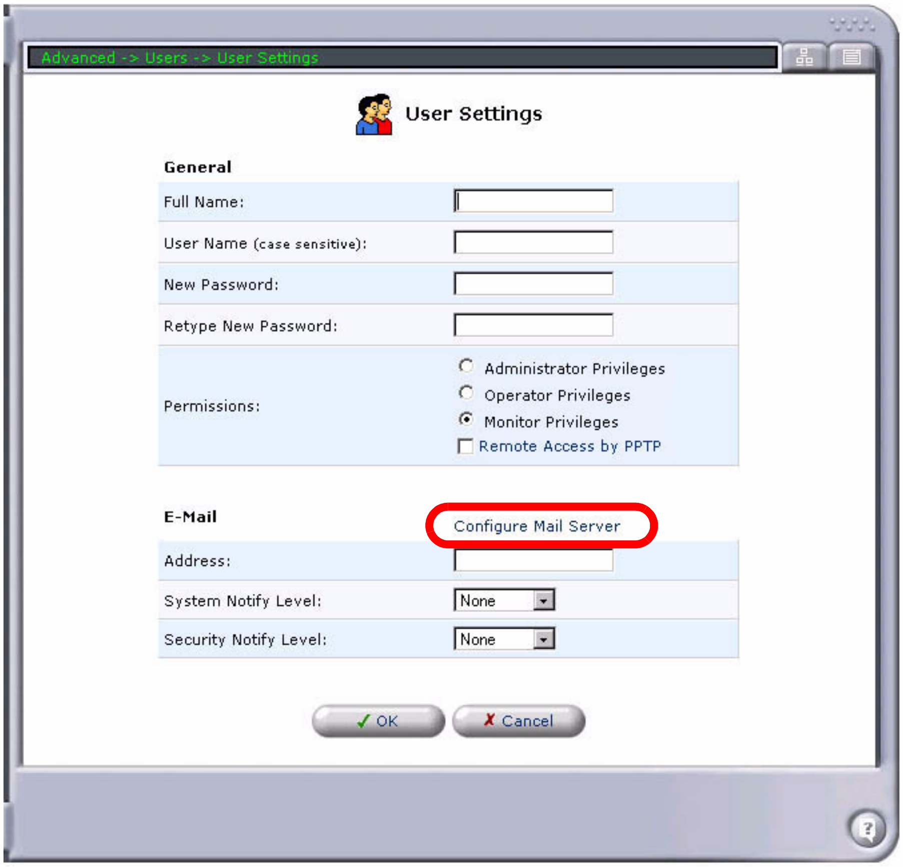
Address:	
System Notify Level:	None
Security Notify Level:	None

4. Select the **OK** button to save.

Configuring E-mail Notification for Users

The e-mail notification feature allows users to receive e-mail notification of system events of a defined type or severity.

1. Select **Advanced/ Users**.
2. If you have not already done so, configure the Outgoing Mail Server. Select **Configure Mail Server**, which opens the System Settings window. See *System Settings* on page 2-57 for information on setting the Mail Server.



Advanced -> Users -> User Settings

User Settings

General

Full Name:	
User Name (case sensitive):	
New Password:	
Retype New Password:	
Permissions:	○ Administrator Privileges ○ Operator Privileges ● Monitor Privileges □ Remote Access by PPTP

E-Mail Configure Mail Server

Address:	
System Notify Level:	None
Security Notify Level:	None

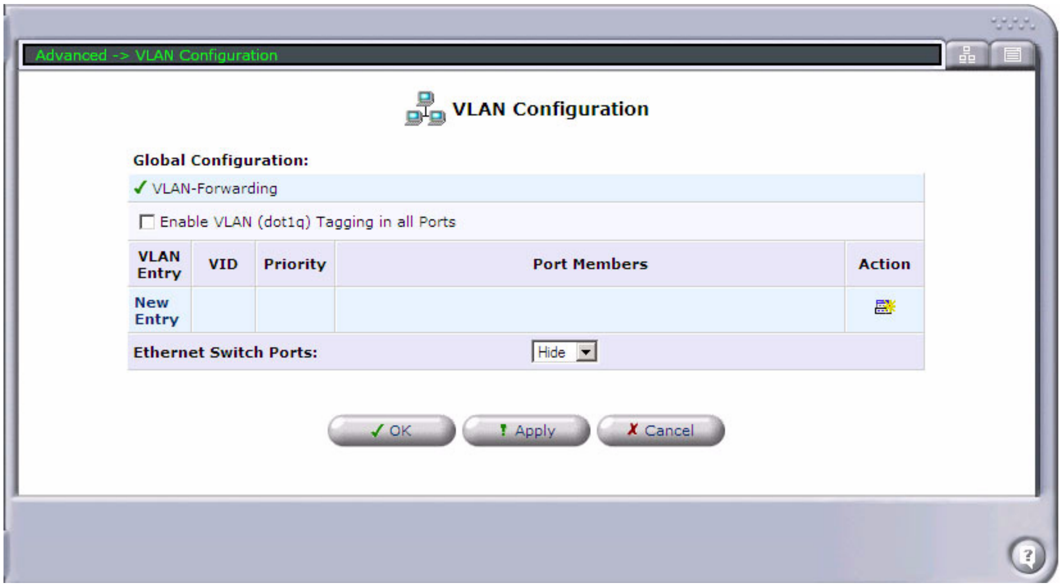
3. Enter the user's e-mail address in the **Address** field.
4. Select the **System** and **Security** levels (Error, Warning, or Information) from the pulldown menus. **Note:** Warning includes Warning and Error notifications.

VLAN Configuration

The Virtual Local Area Network (VLAN) feature provides a way to logically group network devices that are in a Wide Area Network (WAN) and enable them to communicate as if they were in a Local Area Network (LAN). This is a broadcast domain where the members of the domain can be on multiple physical LAN segments.

Creating a VLAN segment requires a VLAN aware switch. The switch can be configured to create different VLAN segments. This allows several VLANs to operate concurrently over a single switch without interfering with each other's broadcast domain, improving the efficiency of the network. VLAN also provides the following benefits to an Enterprise network:

- **Reduced Equipment Cost -** Eliminates the need for expensive routers.
- **Simple Administration -** Moving an end-user is nearly effortless, as the user will be in the same VLAN segment regardless of the physical location.
- **Added Security -** VLANs can be utilized as a firewall. Broadcast messages are within the VLAN and are visible only to the VLAN.



Advanced -> VLAN Configuration

VLAN Configuration

Global Configuration:

✓ VLAN-Forwarding

□ Enable VLAN (dot1q) Tagging in all Ports

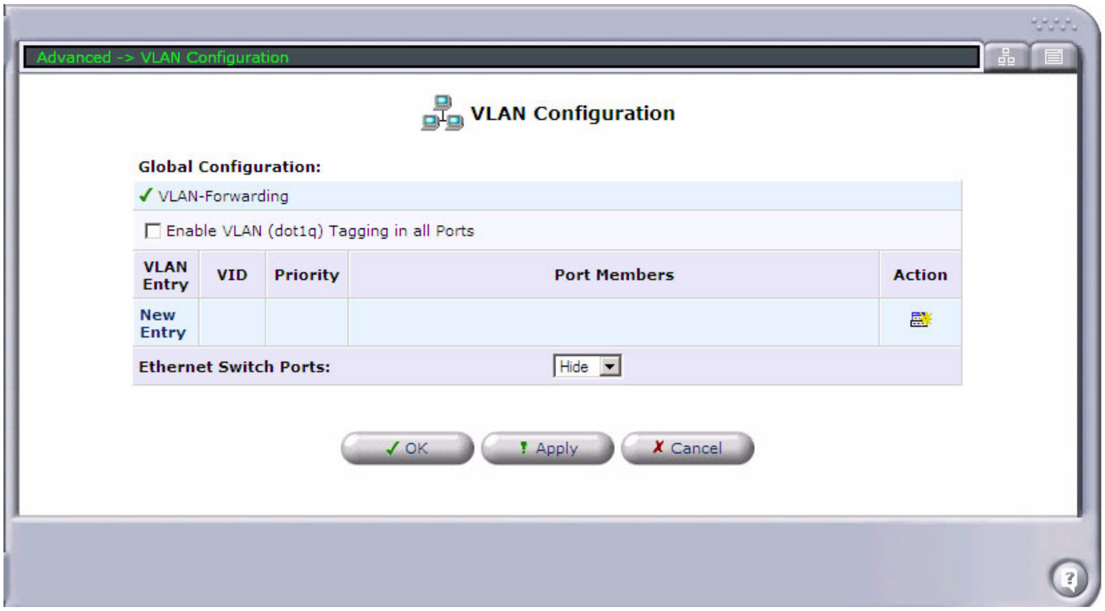
VLAN Entry	VID	Priority	Port Members	Action
New Entry				

Ethernet Switch Ports: Hide

Field	Definition
Global Configuration	**VLAN Forwarding** - Always on. **Enable VLAN (dot1q) Tagging in all Ports** - Enable/disable dot1q tagging.
VLAN Entry	Displays the VLAN entry number.
VID	Displays the VLAN ID number.
Priority	Displays the VLAN priority number.
Port Members	Displays the VLAN Port Members.
New Entry	See the following section for information.
Ethernet Switch Ports	**Show** - Displays the Ethernet Switch ports on this window. **Hide** - Does not display the Ethernet Switch ports. Default.

Configuring a VLAN

1. Select **Advanced/ VLAN Configuration**.



Advanced -> VLAN Configuration

VLAN Configuration

Global Configuration:

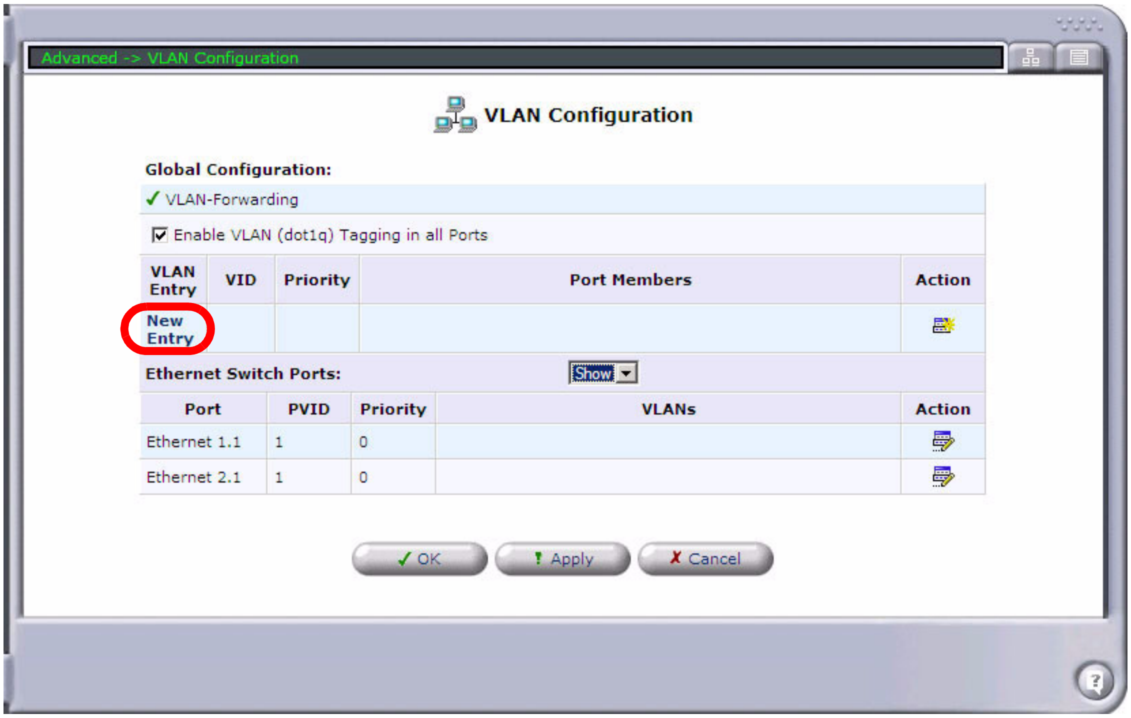
✓ VLAN-Forwarding

□ Enable VLAN (dot1q) Tagging in all Ports

VLAN Entry	VID	Priority	Port Members	Action
New Entry				

Ethernet Switch Ports: Hide

2. Select **Enable VLAN (dot1q) Tagging in all Ports**.
3. Select **New Entry**.



Advanced -> VLAN Configuration

VLAN Configuration

Global Configuration:

✓ VLAN-Forwarding

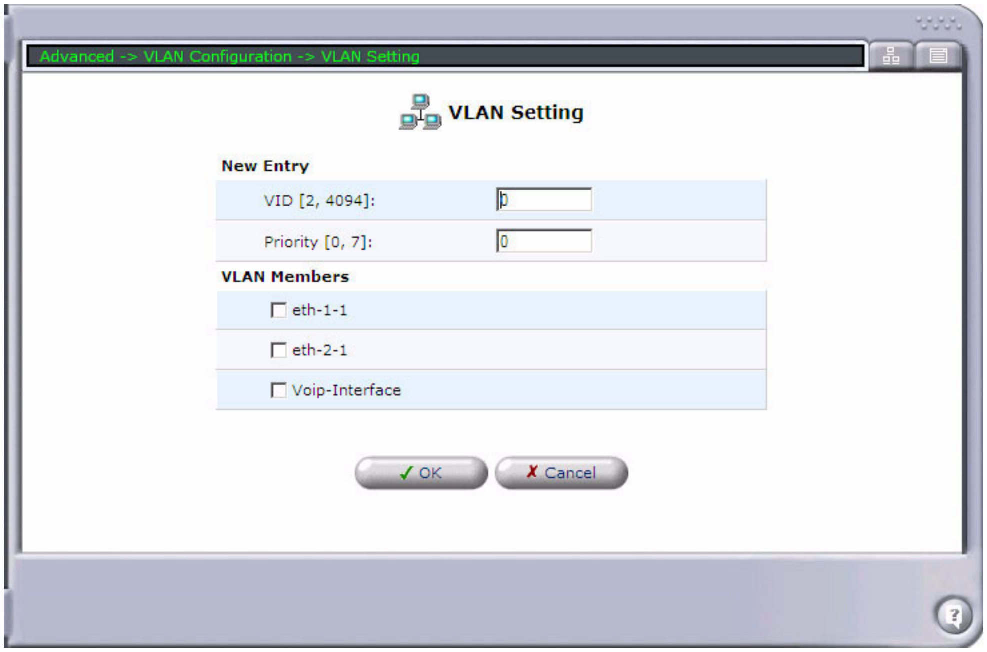
☑ Enable VLAN (dot1q) Tagging in all Ports

VLAN Entry	VID	Priority	Port Members	Action
New Entry				

Ethernet Switch Ports: Show

Port	PVID	Priority	VLANs	Action
Ethernet 1.1	1	0		
Ethernet 2.1	1	0		

4. Enter a **VID** (VLAN ID number) for the VLAN. Range is 2-4094.
5. Set the **Priority** level, if needed. Range is 7-0.
6. Select the **VLAN Members** (Ethernet or VoIP) of this VLAN by checking the associated box. Each port can be a member of up to 4 VLANs. Ports are identified as {port-number}-{sub-interface}.



Advanced -> VLAN Configuration -> VLAN Setting

VLAN Setting

New Entry

VID [2, 4094]:	0
Priority [0, 7]:	0

VLAN Members

□ eth-1-1

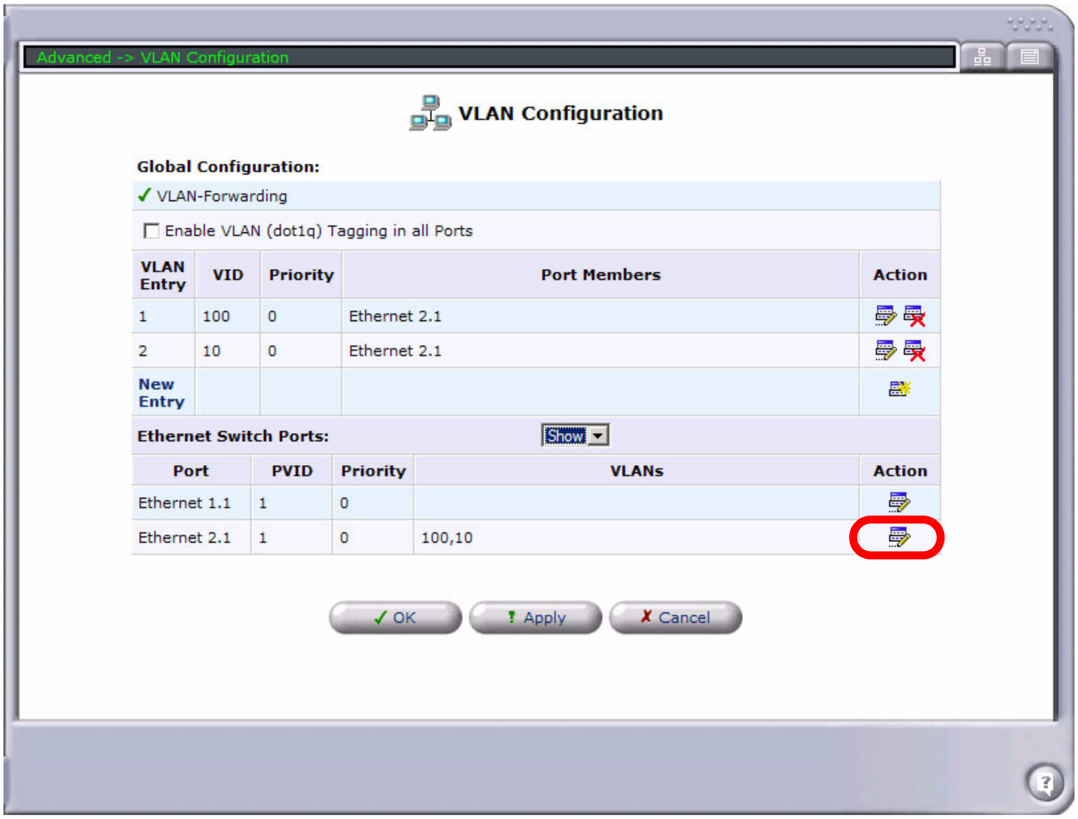
□ eth-2-1

□ Voip-Interface

7. Select **OK**.

Configuring the VLAN Port Setting

1. Select **Advanced/ VLAN Configuration.**
2. Select the VLAN port to configure.



Advanced -> VLAN Configuration

VLAN Configuration

Global Configuration:

✓ VLAN-Forwarding

□ Enable VLAN (dot1q) Tagging in all Ports

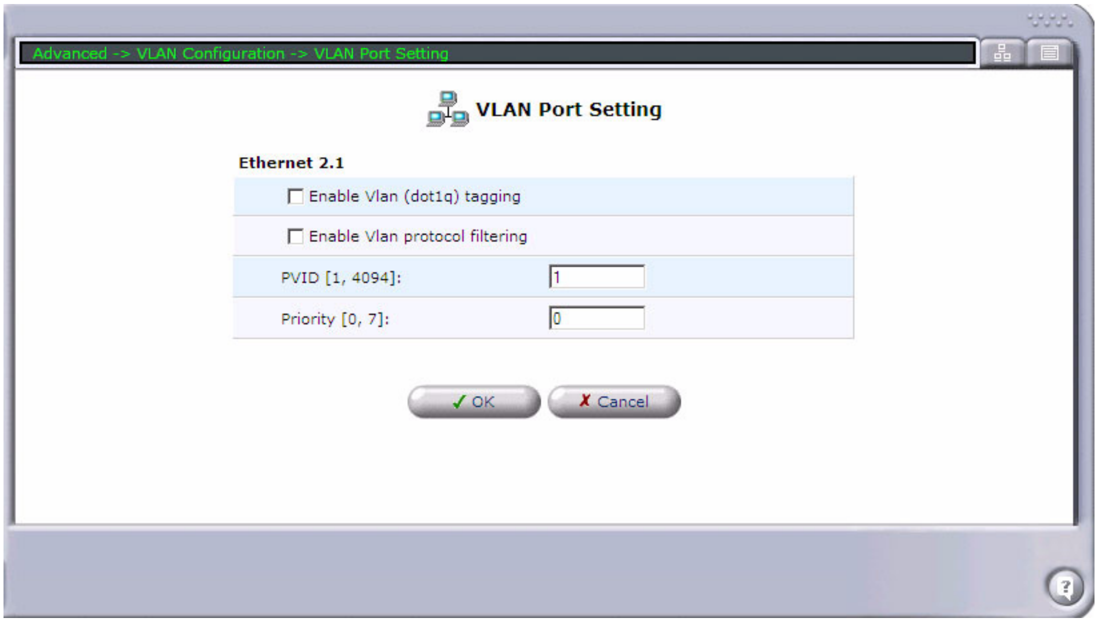
VLAN Entry	VID	Priority	Port Members	Action
1	100	0	Ethernet 2.1	
2	10	0	Ethernet 2.1	
New Entry				

Ethernet Switch Ports: Show

Port	PVID	Priority	VLANs	Action
Ethernet 1.1	1	0		
Ethernet 2.1	1	0	100,10	

3. Configure the port as needed.

Field	Definition
Enable VLAN (dot1q) tagging	This checkbox enables VLAN tagging on this port. Default is disabled (unchecked).
Enable VLAN protocol filtering	This checkbox enables frame filtering on this port. Default is disabled (the frame will go through the normal forwarding/bridging process).
PVID	Port VLAN ID.
Priority	VLAN priority setting. Range is 0-7 (0-2 = low, 3-6 = medium, 7 = high)


Advanced -> VLAN Configuration -> VLAN Port Setting

VLAN Port Setting

Ethernet 2.1

☐ Enable Vlan (dot1q) tagging

☐ Enable Vlan protocol filtering

PVID [1, 4094]: 1

Priority [0, 7]: 0

4. Select **OK** to save changes.

CHAPTER 3

Network Connections

In this Chapter

- Overview
  - Adit 3000 Connections
  - Adit MSR Connections
- Preconfigured Connections
  - Ethernet 1
  - Ethernet 2
  - Serial 1 (Adit 3000 Only)
  - T1 1 - T1 4 (Adit 3000 Only)
- Connections that Require Configuration
  - Multilink
  - Serial (PPPoDS0)
- New Connection
  - Point-to-Point Protocol over DS0 (Serial)
  - Multilink Point-to-Point Protocol over DS0 (Multilink)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Point-to-Point Tunneling Protocol Server (PPTP Server)
  - Layer Two Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPSec)
- OSPF Configuration on the Network Connection

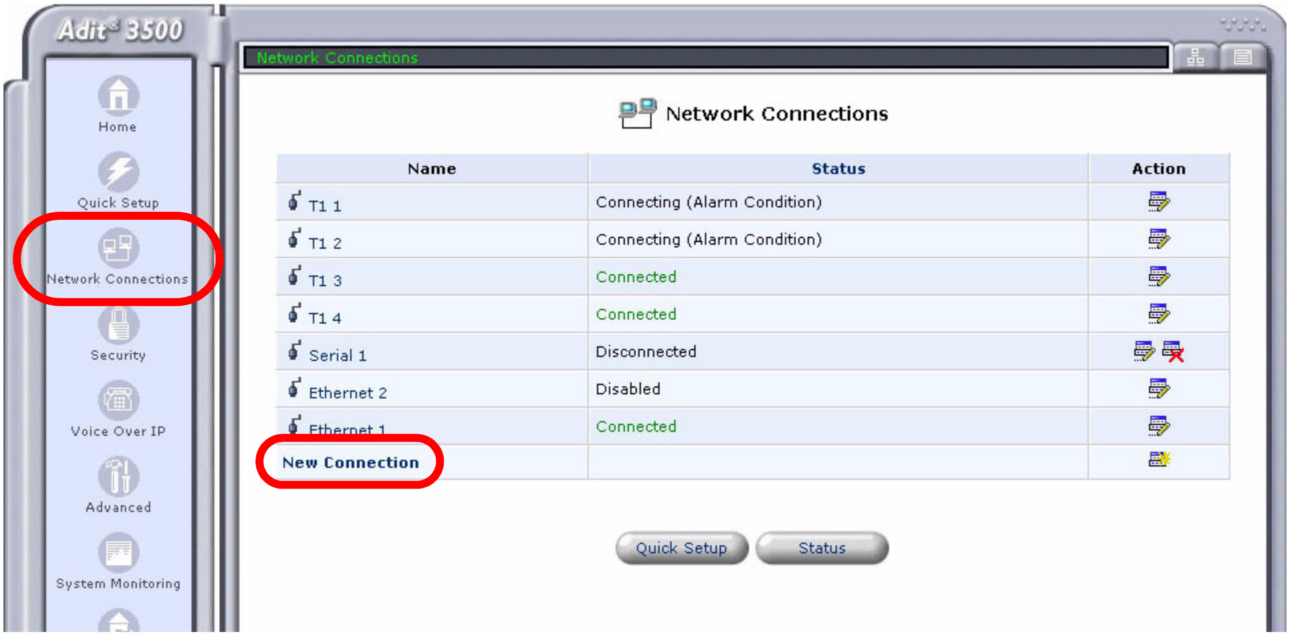
Overview

The Network Connection window allows the user to create and configure network connections. For the Adit 3000, the basic connections for the system are preconfigured. For the Adit MSR, only the Ethernet connections are preconfigured. Additional connections can be set up with the **New Connection** option.

Adit 3000 Connections

When the Adit 3000 boots up, it detects the number of T1s on the configured system and creates the appropriate T1, Ethernet, and Serial connections.

3104	3200	3500	Types	Configuration
Existing (default) Connections				
X	**X**	**X**	T1 1	WAN T1
		X	T1 2	WAN T1. T1 2 is used as the trunk and is configured for PRI-Ni2 signaling/switching.
		X	T1 3	WAN T1
		X	T1 4	WAN T1
X	**X**	**X**	Ethernet 1	LAN Ethernet.
X	**X**	**X**	Ethernet 2	WAN Ethernet (disabled).
X	**X**	**X**	Serial 1 (PPPoT1)	WAN PPPoT1 (disconnected)
New Connections				
X	**X**	**X**	Multilink	Multilink Point-to-Point Protocol over DS0. Connect to the Internet using a MLPPP tunnel over HDLC.
X	**X**	**X**	Serial 1 (PPPoT1)	Point-to-Point Protocol over DS0. Connect to the Internet using a PPP tunnel over HDLC.



Network Connections

Name	Status	Action
T1 1	Connecting (Alarm Condition)	✎
T1 2	Connecting (Alarm Condition)	✎
T1 3	Connected	✎
T1 4	Connected	✎
Serial 1	Disconnected	✎ ✗
Ethernet 2	Disabled	✎
Ethernet 1	Connected	✎
New Connection		✎

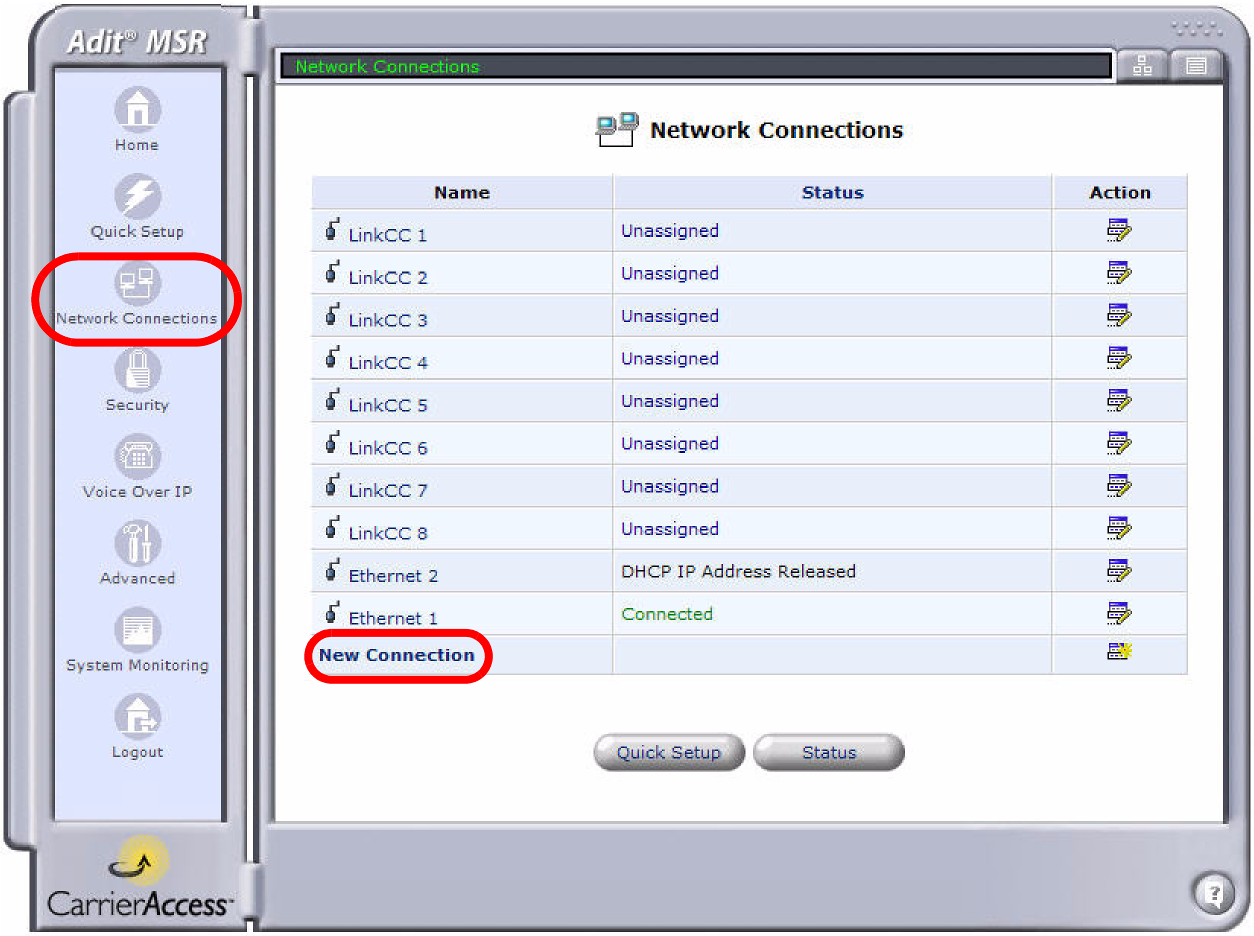
Adit MSR Connections

The MSR provides the following connections:

- **LCC 1-8** – Link Cross-Connects (LCCs) are resources that can be cross-connected to Adit 600 resources. There are three user-configurable types of LCCs:
  - **Data** - Data-typed LCCs are used for PPP or MLPPP WAN links between the MSR card and any available Adit 600 WAN destination, such as T1 lines or WAN-capable cards.
  - **Voice** - Voice-typed LCCs are used for CAS links between MSR CAS trunk functionality and Adit 600 external T1 lines. (E1 to be available in a future release.)
  - **PRI** - PRI-typed LCCs are used for PRI links between MSR PRI trunk functionality and Adit 600 external T1 lines. (E1 to be available in a future release.)
- **Ethernet 1** - LAN Ethernet by default. (Can be configured for WAN usage.)
- **Ethernet 2** - WAN Ethernet by default. (Can be configured for LAN usage.)

The following types of connections can be created with the **New Connection** option:

- **Point-to-Point Protocol over DS0 (Serial)** - Connect to the Internet using a PPP tunnel over HDLC.
- **Multilink Point-to-Point Protocol over DS0 (Multilink)** - Connect to the Internet using a MLPPP tunnel over HDLC.
- **Point-to-Point Tunneling Protocol (PPTP)** - Enable secure transfer of data to another location over the Internet.
- **Point-to-Point Tunneling Protocol Server (PPTP Server)** - Enable Virtual Private Network (VPN) connections to your home network from other locations.
- **Layer Two Tunneling Protocol (L2TP)** - Enable secure transfer of data to another location over the Internet.
- **Internet Protocol Security (IPSec)** - Enable secure transfer of data to another location over the Internet, using private and public keys for encryption, and digital certificates for authentication.



Network Connections

Name	Status	Action
LinkCC 1	Unassigned	
LinkCC 2	Unassigned	
LinkCC 3	Unassigned	
LinkCC 4	Unassigned	
LinkCC 5	Unassigned	
LinkCC 6	Unassigned	
LinkCC 7	Unassigned	
LinkCC 8	Unassigned	
Ethernet 2	DHCP IP Address Released	
Ethernet 1	Connected	
New Connection		

Preconfigured Connections

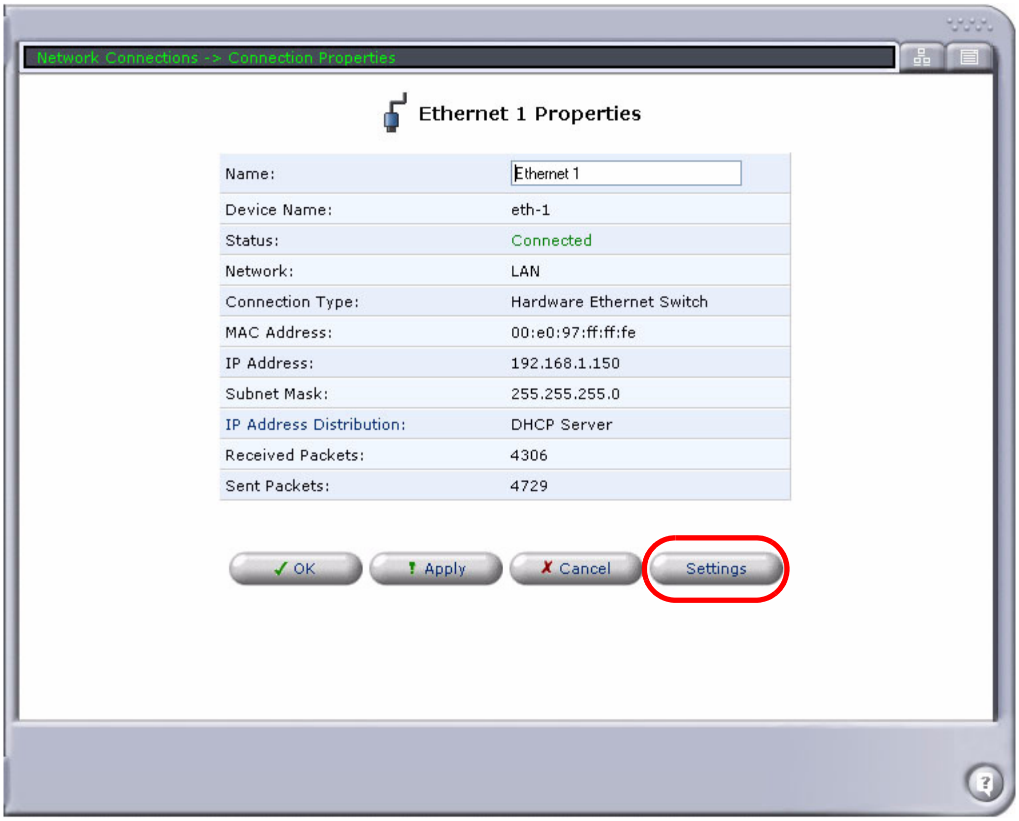
The following connections that may be preconfigured on the system. **Note:** When the system is set back to its default settings, these connections will all be reset to this original configuration.

- **Ethernet 1**
- **Ethernet 2**
- **Serial 1 (Adit 3000 Only)**
- **T1 1 - T1 4 (Adit 3000 Only)**

Ethernet 1

NOTE: For the MSR, DHCP is disabled by default.

For the Adit 3000, Ethernet 1 is automatically configured as the DHCP server. The **Ethernet 1 Properties** window displays the current settings of the connection. This connection is set up as a default, and can be enabled or disabled, but cannot be deleted.


Network Connections -> Connection Properties

Ethernet 1 Properties

Name:	Ethernet 1
Device Name:	eth-1
Status:	Connected
Network:	LAN
Connection Type:	Hardware Ethernet Switch
MAC Address:	00:e0:97:ff:ff:fe
IP Address:	192.168.1.150
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Received Packets:	4306
Sent Packets:	4729

Configuring Ethernet 1

To change the configuration of Ethernet 1, select the **Settings** button and modify the settings as necessary. Select **Apply** when finished. The following are the field definitions for the Ethernet 1 settings:

Field	Definition
General	
Device Name	Displays the device name.
Status	Displays the current status (Disabled, Connected, ...)
Schedule Availability	Defines when the LAN is available. The default is **Always**. To create a Schedule Availability rule, click **New**.
Network	Defines the type of network: **WAN** - Wide Area Network **LAN** - Local Area Network (Default). **DMZ** - Demilitarized Zone
Connection Type	Displays connection type (Hardware Ethernet Switch).
Speed/Duplex	Sets the speed and duplex behavior for the Ethernet interface: **Auto** - Auto-negotiate the speed and duplex for the interface. Default. **100T-FD** - 100 Mbps speed and full-duplex. **100T-HD** - 100 Mbps speed and half-duplex. **10T-FD** - 10 Mbps speed and full-duplex. **10T-HD** - 10 Mbps speed and half-duplex.
Internet Protocol (For the Adit 3000, this name is a link to the *Advanced/IP Address Distribution (DHCP)* window.)	
Obtain an IP Address Automatically	Sets the connection to use DHCP to obtain an IP address. **Override Subnet Mask** - Set specific mask. **DHCP Option Auto Provision** - Enable DHCP auto provisioning. **Rx TOS Marking** - Enable IP TOS marking. **Rx TOS Value** - Hex value, range 0x00-0xFF, default is 0x00
Use the Following IP Address	**IP Address** - Sets the IP Address **Subnet Mask** - Sets the Subnet of the IP Address **Default Gateway** - Sets the Default Gateway IP Address. **Rx TOS Marking** - Enable IP TOS marking. **Rx TOS Value** - Hex value, range 0x00-0xFF, default is 0x00
DNS Static Entries (This name is a link to the *Advanced/DNS Static Entries* window.) **Note:** This field appears when Internet Protocol is set to "Obtain an IP Address Automatically"	
Primary DNS Server	The IP address of the primary DNS server, in the form of xxx.xxx.xxx.xxx, where xxx is between 0-255.
Secondary DNS Server	The IP address of the secondary DNS server, in the form of xxx.xxx.xxx.xxx, where xxx is between 0-255.

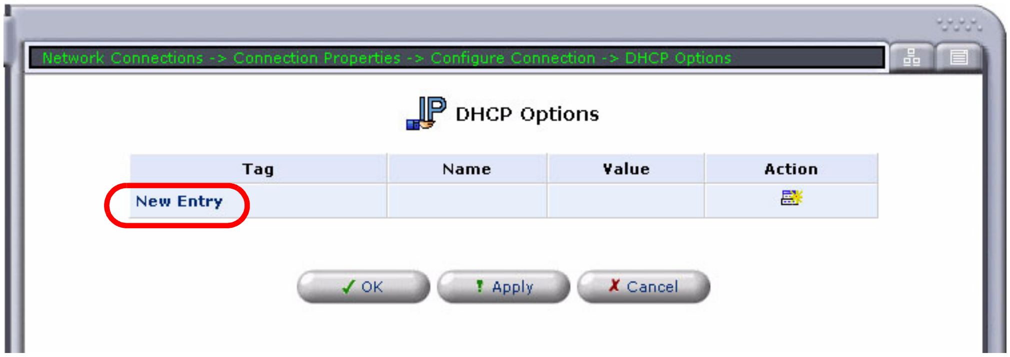
Field	Definition (Continued)
IP Address Distribution (This name is a link to the *Advanced/IP Address Distribution (DHCP)* window.)	
Disabled	Disables this feature.
DHCP Server	Configures DHCP Server. **Start IP Address** - Client address pool starting address **End IP Address** - Client address pool ending address **Subnet Mask** - Subnet mask of the Start/End IP address listed above. **WINS Server IP Address** - Windows Internet Name Service Server IP address. **Lease Time In Minutes** - lease during the DHCP server applies to the client assignments. **Provide Host Name if Not Specified by Client** - Select to enable.
DHCP Relay	**New IP Address** - The address of the DHCP Relay Server.
DHCP Options	Opens a window that configures the DHCP options per RFC 2132. See *Configuring DHCP Options* on page 3-8.
Routing (This name is a link to the *Advanced/Routing* window)	
Routing Mode	Displays the current routing mode.
Device Metric	Value of Metric of IP network on this interface in Routing Table. Range is 0-255.
Default Route	Check to enable default route.
Proxy ARP - Ethernet ARP Proxy	Check to enable Proxy ARP.
Routing Protocol	**None -** Disable the routing protocol on this interface. **OSPF** - Set the routing protocol to OSPF on this interface. There is a link below the option to configure OSPF. **RIP** - Set the routing protocol to RIP on this interface. **Listen to RIP Messages** - None, RIPv1, RIPv2, RIPv1/2 **Send RIP Messages** - None, RIPv1, RIPv2 - Broadcast, RIPv2 - Multicast
Internet Connection Firewall	**Note:** This name is a link to the *Security* window. Enables/Disables Firewall for this device.
Allow Unrestricted Administration	**Note:** This name is a link to the *Security* window. Enables/disables unrestricted administration.
Additional IP Addresses	**New IP Address** - Opens a window to assign an additional IP address to this device.

NOTE: For a manually specified network mode (Internet Protocol: Use the following IP address), the default route does not get installed until both the **Default Route** checkbox is enabled AND the user has entered a valid non-0.0.0.0 Gateway IP in the **Default Gateway** field.

Configuring DHCP Options

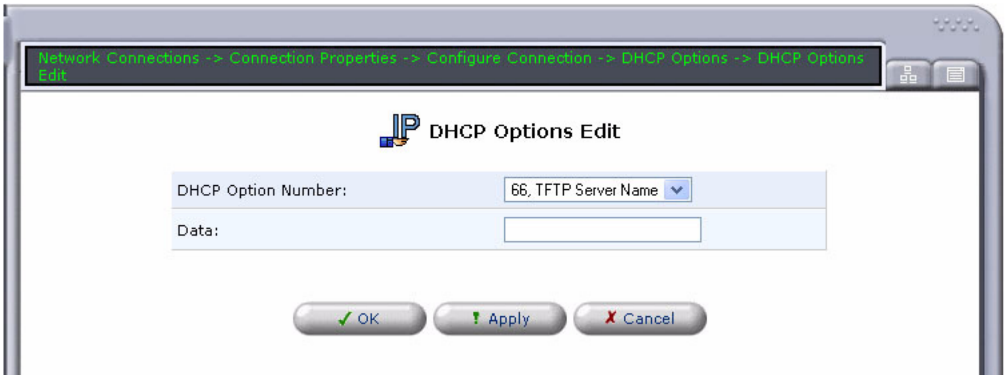
To configure DHCP options:

1. From the Configure Ethernet 1 window, select **DHCP Server** for IP Address Distribution.
2. Select the **DHCP Options** field.
3. Select **New Entry**.


Network Connections -> Connection Properties -> Configure Connection -> DHCP Options
DHCP Options
✓ OK
! Apply
✗ Cancel

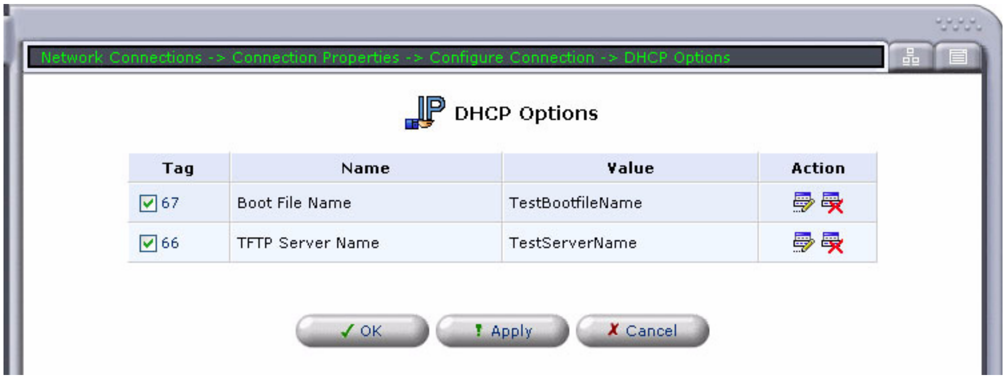
Tag	Name	Value	Action
New Entry			

4. At the **DHCP Option Number** pulldown field, select one of the following:
   - 66, TFTP Server Name
   - 67, Boot File Name


Network Connections -> Connection Properties -> Configure Connection -> DHCP Options -> DHCP Options Edit
DHCP Options Edit
✓ OK
! Apply
✗ Cancel

DHCP Option Number:	66, TFTP Server Name
Data:	

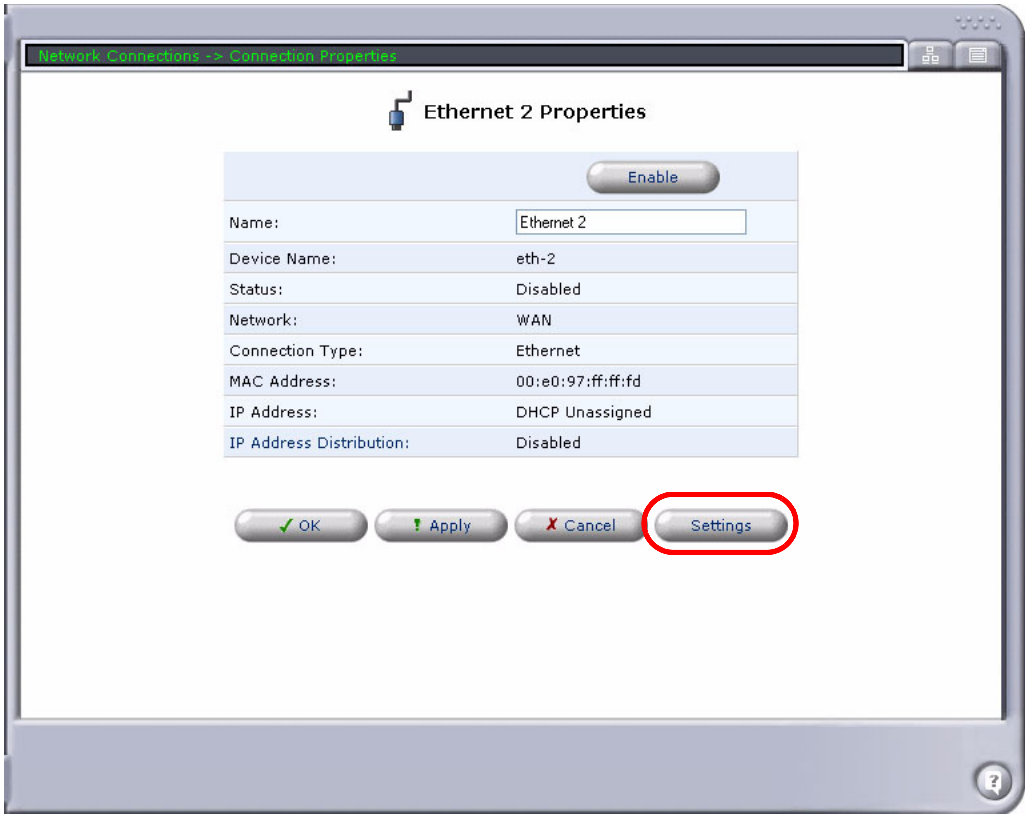
5. On the **Data** field enter the IP address or host name.
6. Select **OK**. The information appears in the DHCP Options table.


Network Connections -> Connection Properties -> Configure Connection -> DHCP Options
DHCP Options
✓ OK
! Apply
✗ Cancel

Tag	Name	Value	Action
☑ 67	Boot File Name	TestBootfileName	
☑ 66	TFTP Server Name	TestServerName	

Ethernet 2

The **Ethernet 2 Properties** window displays the current settings of the connection. This connection is set up as a default, and can be enabled or disabled, but cannot be deleted.



Ethernet 2 Properties

Name:	Ethernet 2
Device Name:	eth-2
Status:	Disabled
Network:	WAN
Connection Type:	Ethernet
MAC Address:	00:e0:97:ff:ff:fd
IP Address:	DHCP Unassigned
IP Address Distribution:	Disabled

Configuring Ethernet 2

To change the configuration of Ethernet 2, select the **Settings** button and modify the settings as necessary. Select **Apply** when finished. The following are the field definitions for the Ethernet 2 settings:

Field	Definition
General	
Device Name	Displays the device name.
Status	Displays the current status (Disabled, Connected, ...).
Schedule Availability	Defines when the WAN is available. The default is **Always**. To create a Schedule Availability rule, click **New**.
Network	Defines the type of network: **WAN** - Wide Area Network (Default). **LAN** - Local Area Network **DMZ** - Demilitarized Zone
Connection Type	Displays the connection type (Ethernet).
MTU	Maximum Transmission Unit. Sets the largest packet size (bytes) the network will transmit: **Automatic** at 1500. **Manual** at a range of 576 to 1500.
Speed/Duplex	Sets the speed and duplex behavior for the Ethernet interface: **Auto** - Auto-negotiate the speed and duplex for the interface. Default. **100T-FD** - 100 Mbps speed and full-duplex. **100T-HD** - 100 Mbps speed and half-duplex. **10T-FD** - 10 Mbps speed and full-duplex. **10T-HD** - 10 Mbps speed and half-duplex.
Internet Protocol	
Obtain an IP Address Automatically	Sets the connection to use DHCP to obtain an IP address. **Override Subnet Mask** - Set specific mask. **DHCP Option Auto Provision** - Enable DHCP auto provisioning. **Rx TOS Marking** - Enable IP TOS marking. **Rx TOS Value** - Hex value, range 0x00-0xFF, default is 0x00
Use the Following IP Address	**IP Address** - Sets the IP Address **Subnet Mask** - Sets the Subnet of the IP Address **Default Gateway** - Sets the Default Gateway IP Address. **Rx TOS Marking** - Enable IP TOS marking. **Rx TOS Value** - Hex value, range 0x00-0xFF, default is 0x00
DNS Static Entries (this name is a link to the *Advanced/DNS Static Entries* window) **Note:** This field appears when Internet Protocol is set to Obtain an IP Address Automatically	
Obtain DNS Server Address Automatically	To automatically obtain the DNS Server Address.
Use the Following DNS Server Addresses	**Primary DNS Server** - Enter the specific DNS server address to use. **Secondary DNS Server** - Enter a secondary DNS server address to use.

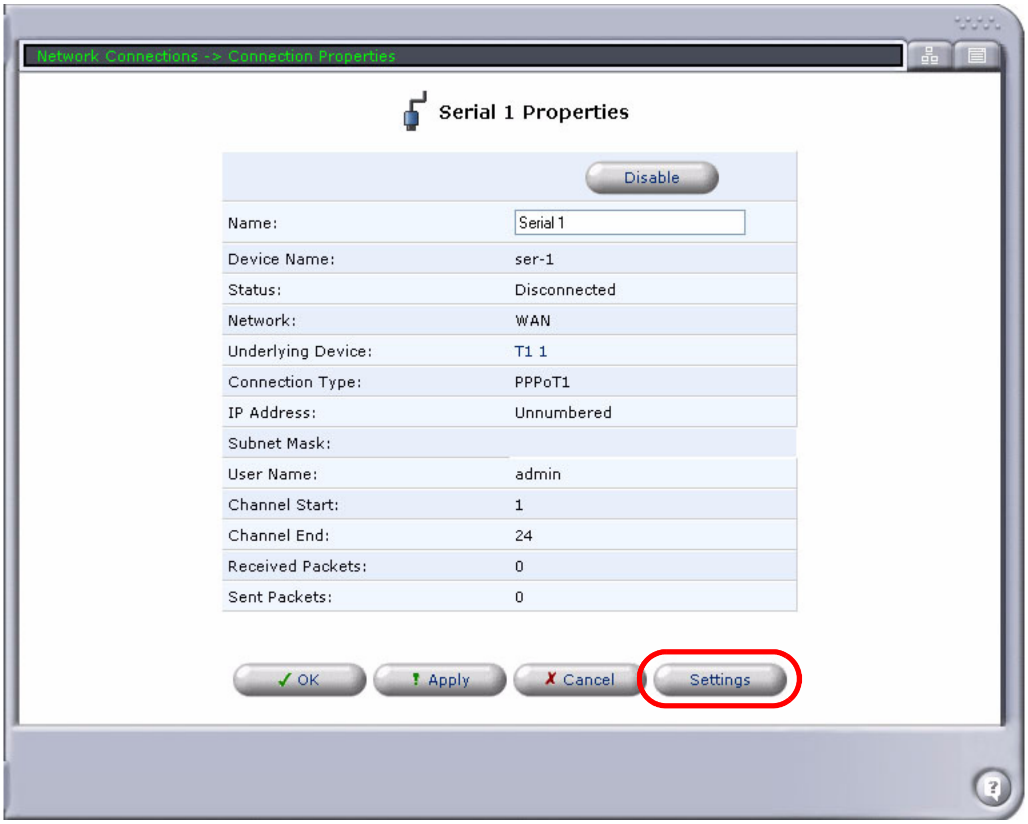
Field	Definition (Continued)
IP Address Distribution (This name is a link to the *IP Address Distribution (DHCP)* window.*)*	
Disabled	Disables address distribution. Default.
DHCP Server	Configures DHCP Server. **Start IP Address -** Starting address of the client address pool **End IP Address -** Ending address of the client address pool **Subnet Mask -** Subnet mask of the Start/End IP address listed above. **WINS Server IP Address** - Windows Internet Name Service Server IP address. **Lease Time In Minutes -** Lease during that the DHCP server applies to the client assignment.s **Provide Host Name if Not Specified by Client** - Check to enable.
DHCP Relay	**New IP Address -** Opens a new window. Enter the address of the DHCP Relay Server.
Routing (This name is a link to the *Advanced*/*Routing* window.)	
Routing Mode	Display/edit the routing mode. **Route -** Routing is used if public is visible on both sides. **NAPT -** Default. NAPT is used if doing private IPs on the Ethernet side or if you want to hide specific publics on the internal side.
SIP ALG	**Note:** This field only applies when the **Routing Mode** is set to **NAPT**. This field allows the customer to turn off the SIP ALG on external interfaces. **Checked** - the SIP ALG will be switched off. **Unchecked** - the SIP ALG will not work.
Device Metric	Value of Metric of IP network on this interface in the Routing Table. Range is 0-255.
Default Route	Check to enable default route.
Proxy ARP - Ethernet ARP Proxy	Check to enable Proxy ARP.
Routing Protocol	**None -** Disable the routing protocol on this interface. **OSPF** - Set the routing protocol to OSPF on this interface. There is a link below the option to configure OSPF. **RIP** - Set the routing protocol to RIP on this interface. **Listen to RIP Messages** - None, RIPv1, RIPv2, RIPv1/2 **Send RIP Messages** - None, RIPv1, RIPv2 - Broadcast, RIPv2 - Multicast
Internet Connection Firewall	**Note:** This name is a link to the *Security* window Enables/Disables Firewall for this device.
Additional IP Addresses	Opens a window to add an additional IP address with subnet mask.

NOTE: For a manually specified network mode (Internet Protocol: Use the following IP address), the default route does not get installed until both the **Default Route** checkbox is enabled AND the user has entered a valid non-0.0.0.0 Gateway IP in the **Default Gateway** field.

Serial 1 (Adit 3000 Only)

The Serial 1 (PPPoDS0) Properties window will display the current settings of the connection., and can be enabled, disabled, deleted or modified from this window.

This is a preconfigured connection on the Adit 3000, however, this is the only preconfigured connection that can be deleted and a new Serial 1 connection can be created based on a different T1. See *New Connection Window* on page 3-28 for information on creating this connection.



Name:	Serial 1
Device Name:	ser-1
Status:	Disconnected
Network:	WAN
Underlying Device:	T1 1
Connection Type:	PPPoT1
IP Address:	Unnumbered
Subnet Mask:	
User Name:	admin
Channel Start:	1
Channel End:	24
Received Packets:	0
Sent Packets:	0

Note: See *Serial (PPPoDS0)* on page 3-21 for information on these windows.

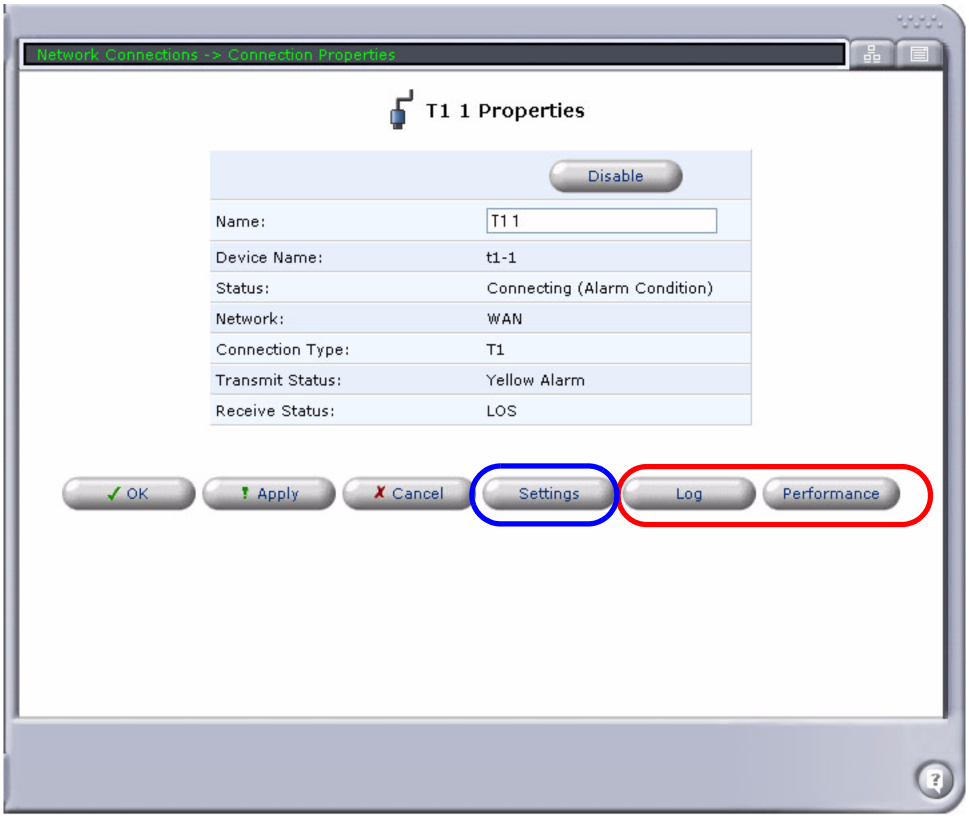
T1 1 - T1 4 (Adit 3000 Only)

There can be up to four preconfigured T1 connections on the Adit 3000. To view/modify the configuration, click on the T1 *n* name on the Network Connections window. This will open the T1 Properties window, which displays the basic information on the T1.

- Name (T1 1, T1 2, T1 3 or T1 4 are default names, they can be modified)
- Device Name (T1 1, T1 2, T1 3 or T1 4)
- Status
- Network (LAN/WAN)
- Connection Type (T1)
- Transmit Status
- Receive Status

The T1 Properties window has two additional buttons:

- **Log** - The Log button links to the System Monitoring/T1 Log window. See *T1 Log (Adit 3000 Only)* on page 5-7 for detailed information.
- **Performance** - The Performance button links to the System Monitoring/T1 #n Performance window. See *T1 Performance (Adit 3000 Only)* on page 5-10 or detailed information.


Network Connections -> Connection Properties

T1 1 Properties

Name:	T1 1
Device Name:	t1-1
Status:	Connecting (Alarm Condition)
Network:	WAN
Connection Type:	T1
Transmit Status:	Yellow Alarm
Receive Status:	LOS

Configuring a T1 (1-4)

The Configure T1 n (1-4) window displays all of the T1 configuration parameters and the default settings for each. To configure a T1, select the **Settings** button, the Configuration window will display. Field definitions for this window are as follows:

Field	Definition
General	
Device Name	Displays the device name (t1-n).
Status	Displays the current status.
Schedule Availability	Defines when the T1 is available. An additional window will open to create a Schedule Availability rule, which will then display in the pulldown selection. Default is **Always**.
Connection Type	Displays connection type (T1).
T1 Configuration	
Circuit Identifier	Display/edit the Circuit ID, default is Adit 3000.
Framing Type	**ESF** - To Extended Superframe (ESF) framing. **D4** - To D4 Superframe (SF) framing.
Line Coding	**Alternate Mark Inversion line coding (AMI)** **Binary 8 Zero Substitution line coding (B8ZS) -** Default
Loop Code Detection	**Enable detection of CSU loop codes** **Enable detection of NIU loop codes** **Off** - Default
Facilities Data Link	**None -** Disable FDL output messages. Default. **T1.403 FDL -** Enable T1.403 FDL performance messages. **fdlPMMsg -** Enable FDL Performance Monitoring messages.
Line Build Out	Sets the DS1 Line Build Out (LBO). DSX-1 equalization for 0-133ft - Default DSX-1 equalization for 133-266ft DSX-1 equalization for 266-399ft DSX-1 equalization for 399-533ft DSX-1 equalization for 533-655ft CSU attenuation for LBO of -7.5dB CSU attenuation for LBO of -15dB CSU attenuation for LBO of -22.5dB
Apply loopback to DS1 interface	**None (loopback disabled) -** Disable loopback. Default **Line loopback enabled -** Apply line loopback. **Payload loopback enabled -** Apply payload loopback.
Idle Pattern	A hexadecimal number with a range from 0x00 to 0xff. This number must be preceeded by 0x.

Field	Definition (Continued)	
Threshold Settings	**Daily (default)**	**15 Minute (default)**
Bursty Errored Seconds Defect Threshold (BES)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900
Controller Slip Seconds Defect Threshold (CSS)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900
Degraded Minutes Threshold (DM)	Default is 0. Range is 0 - 1440	Default is 0. Range is 0 - 15
Errored Seconds Defect Threshold (ES)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900
Line Code Violations Defect Threshold (LCV)	Default is 0. Range is 0 - 133401600	Default is 0. Range is 0 - 1389600
Line Errored Seconds Defect Threshold (LES)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900
Path Code Violation Defect Threshold (PCV)	Default is 0. Range is 0 - 133401600	Default is 0. Range is 0 - 1389600
Severely Errored Frame Seconds Threshold (SEFS)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900
Severely Errored Seconds Threshold (SES)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900
Unavailable Seconds Defect Threshold (UAS)	Default is 0. Range is 0 - 86400	Default is 0. Range is 0 - 900

Log Button

See, System Monitoring/*T1 Log (Adit 3000 Only)* on page 5-7.

Performance Button

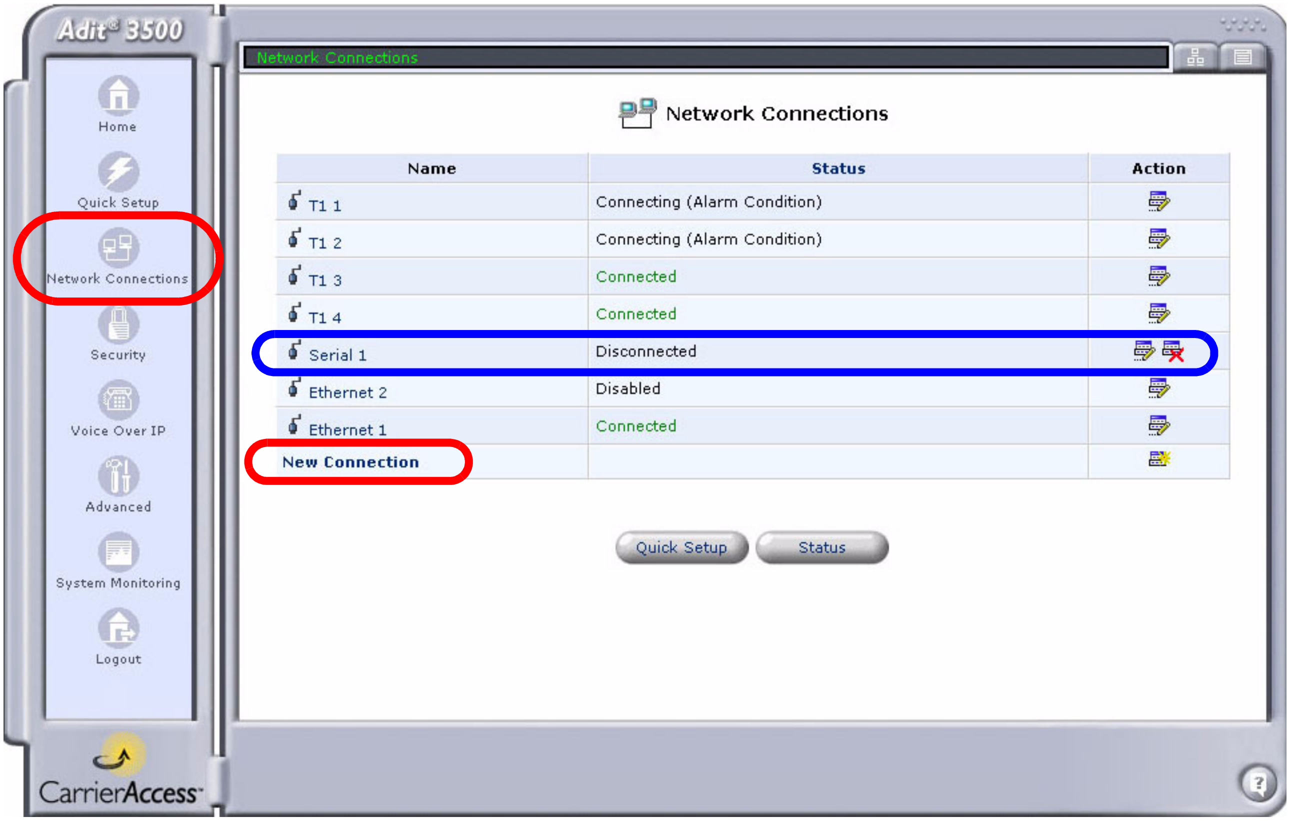
See, System Monitoring/*T1 Performance (Adit 3000 Only)* on page 5-10.

Connections that Require Configuration

The following connection types must be configured using the **New Connection** selection.

- **Multilink**
- **Serial (PPPoDS0)**

NOTE: For the Adit 3000, you must first deleted the pre-configured **Serial 1** connection before adding either of these connection types. (For the MSR, there is no pre-configured **Serial 1** connection.)



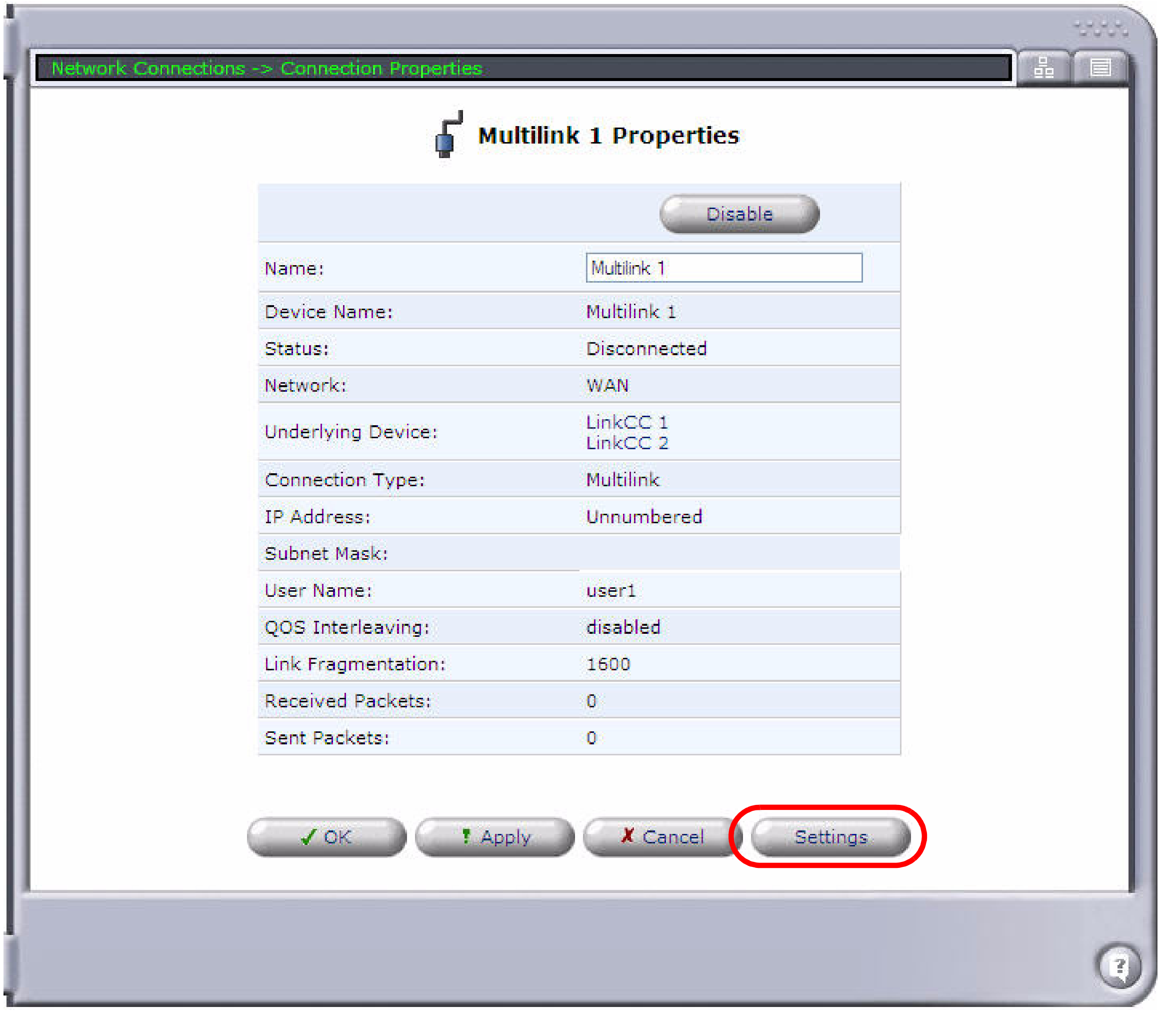
Network Connections

Name	Status	Action
T1 1	Connecting (Alarm Condition)	✎
T1 2	Connecting (Alarm Condition)	✎
T1 3	Connected	✎
T1 4	Connected	✎
Serial 1	Disconnected	✎ ✗
Ethernet 2	Disabled	✎
Ethernet 1	Connected	✎
New Connection		✎

Multilink

The Multilink Properties window displays the settings of a Multilink PPP over DS0 connection configured with the **New Connection** option. (See *New Connection* on page 3-27.) Once the connection is configured, you can select the connection to view its properties, modify its settings, or disable/enable it.

A sample Multilink Properties window for the Adit MSR is shown below. Note that the **Underlying Devices** are LCCs. For the Adit 3000, the **Underlying Devices** are T1s.

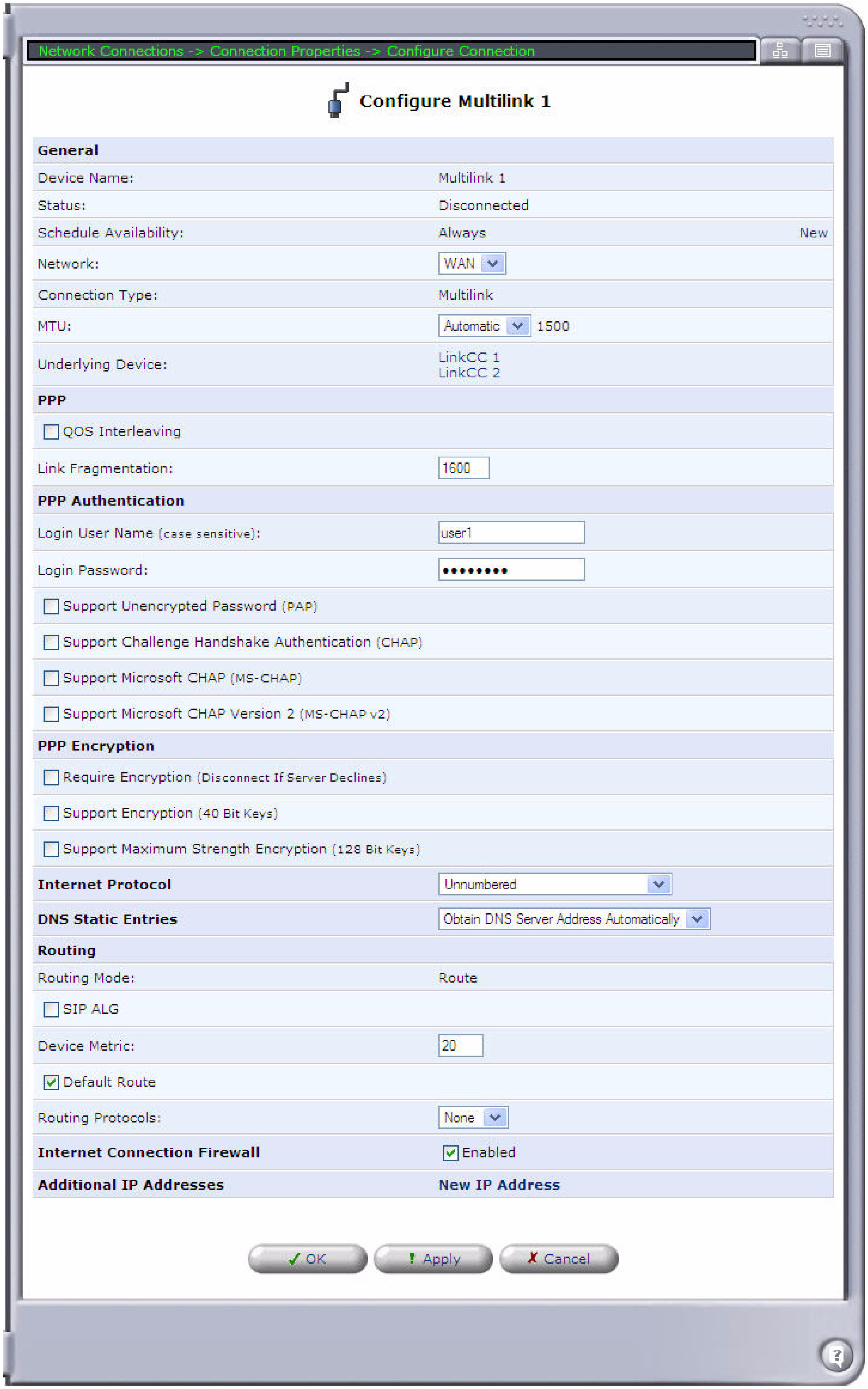


Network Connections -> Connection Properties

Multilink 1 Properties

	Disable
Name:	Multilink 1
Device Name:	Multilink 1
Status:	Disconnected
Network:	WAN
Underlying Device:	LinkCC 1 LinkCC 2
Connection Type:	Multilink
IP Address:	Unnumbered
Subnet Mask:	
User Name:	user1
QOS Interleaving:	disabled
Link Fragmentation:	1600
Received Packets:	0
Sent Packets:	0

If necessary, you can modify the multilink connection by selecting the **Settings** button. The **Configure Multilink 1** window appears, as shown in the following figure.



Network Connections -> Connection Properties -> Configure Connection

Configure Multilink 1

General		
Device Name:	Multilink 1	
Status:	Disconnected	
Schedule Availability:	Always	New
Network:	WAN	
Connection Type:	Multilink	
MTU:	Automatic 1500	
Underlying Device:	LinkCC 1 LinkCC 2	
PPP		
□ QOS Interleaving		
Link Fragmentation:	1600	
PPP Authentication		
Login User Name (case sensitive):	user1	
Login Password:	••••••••	
□ Support Unencrypted Password (PAP)		
□ Support Challenge Handshake Authentication (CHAP)		
□ Support Microsoft CHAP (MS-CHAP)		
□ Support Microsoft CHAP Version 2 (MS-CHAP v2)		
PPP Encryption		
□ Require Encryption (Disconnect If Server Declines)		
□ Support Encryption (40 Bit Keys)		
□ Support Maximum Strength Encryption (128 Bit Keys)		
Internet Protocol	Unnumbered	
DNS Static Entries	Obtain DNS Server Address Automatically	
Routing		
Routing Mode:	Route	
□ SIP ALG		
Device Metric:	20	
☑ Default Route		
Routing Protocols:	None	
Internet Connection Firewall	☑ Enabled	
Additional IP Addresses	**New IP Address**	

The following are field definitions for the **Configure Multilink 1** window:

Field	Definition
General	
Device Name	Displays the device name.
Status	Displays the current status.
Schedule Availability	Defines when the WAN is available. The default is **Always**. To create a Schedule Availability rule, click **New**.
Network	Defines the network type: **WAN** - Wide Area Network (Default). **LAN** - Local Area Network **DMZ** - Demilitarized Zone
Connection Type	Displays the connection type (Multilink).
MTU	Maximum Transmission Unit. Sets the largest packet size (bytes) the network will transmit: **Automatic** at 1500 **Manual** at a range of 576 to 1500.
Underlying Device	Displays the device(s)/connection(s) required for this interface: **Adit 3000:** Lists the T1(s) in this connection. These are links to the High Speed Serial Configuration window. See *Underlying Device - High Speed Serial Configuration (Adit 3000 Only)* on page 3-25. **Adit MSR:** Lists the LCC(s) in this connection.
PPP	
QOS Interleaving	Enables Interleaving. The QoS Interleaving is used when there are QoS considerations with voice or data. Packets are split with a low ToS precedence.
Link Fragmentation	Sets the threshold byte size of the packet for Interleaving. Range is 320 - 1600, with a default of 1600. If the packet is ≥ the set threshold, the packet will be split in half and sent.
PPP Authentication	
Login User Name	Enter Login User Name, with a maximum of 100 characters.
Login Password	Enter login password. Select to enable support of the following: **Support Unencrypted Password (PAP)** **Support Challenge Handshake Authentication (CHAP)** **Support Microsoft CHAP (MS-CHAP)** **Support Microsoft CHAP Version 2 (MS-CHAPv2)**
PPP Encryption	The following PPP encryption can be enabled by checking the boxes: **Require Encryption** (Disconnect if server declines) **Support Encryption** (40 bit keys) **Support Maximum Strength Encryption** (128 bit keys)

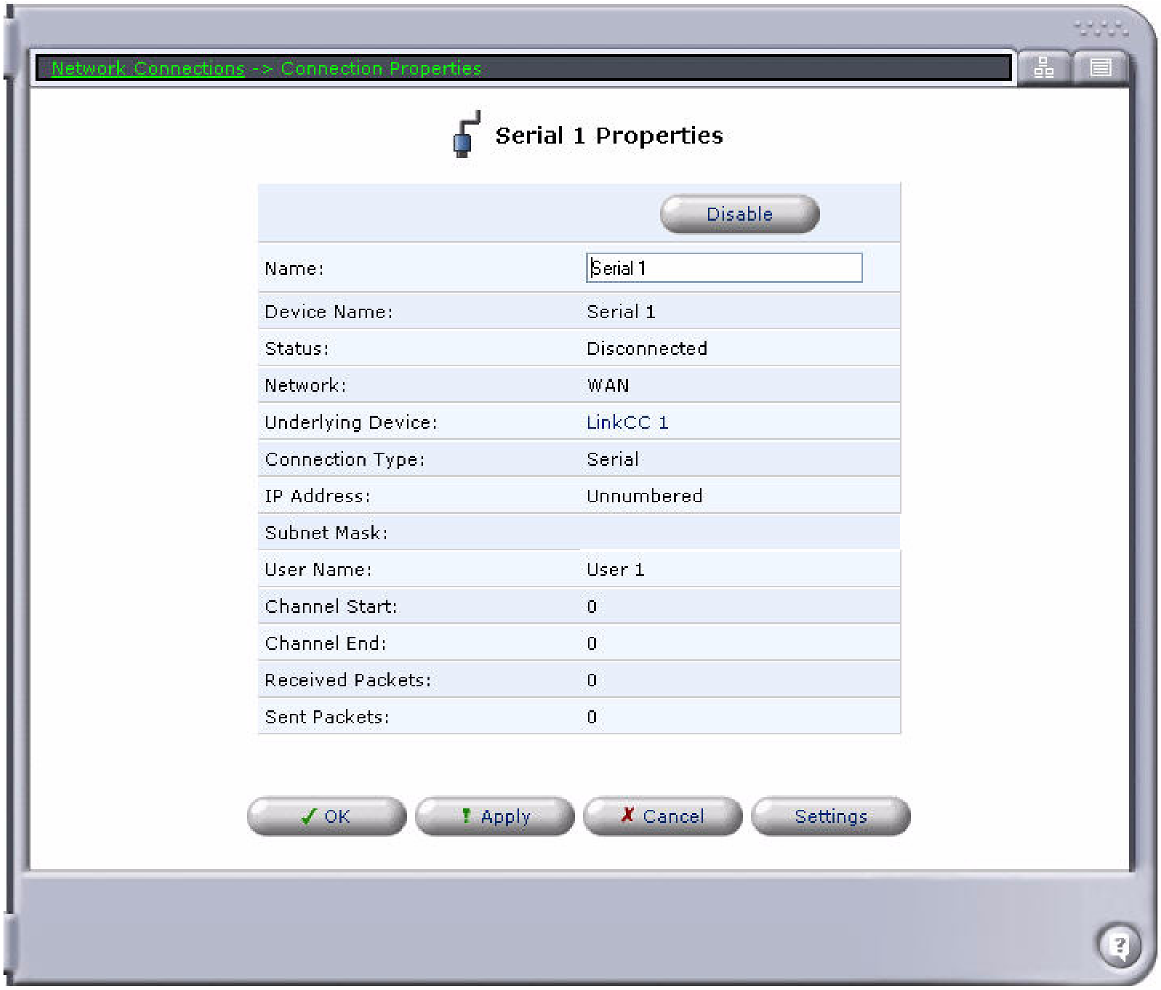
Field	Definition (Continued)
Internet Protocol	
Unnumbered	Treat this as an un-numbered interface, as per RFC 1812.
Obtain an IP Address Automatically	Sets the WAN to use DHCP to obtain an IP address. **Override Subnet Mask** - Set mask, override any previous setting.
Use the Following IP Address	**IP Address** - Sets the IP Address **Override Subnet Mask** - Set mask, override any previous setting.
DNS Static Entries (This name is a link to the *Advanced/DNS Static Entries* window.)	
Obtain DNS Server Address Automatically	Sets the interface to obtain a DNS Server address.
Use the Following DNS Server Address	Sets the DNS Server Address. **Primary DNS Server** - Enter the specific DNS server address to use. **Secondary DNS Server** - Enter a secondary DNS server address to use.
Routing	
Routing Mode	Displays the current routing mode. **Route -** Routing is used if public is visible on both sides. **NAPT -** NAPT is used if doing private IPs on the Ethernet side or if you want to hide specific publics on the internal side.
SIP ALG	This field allows the customer to turn off the SIP ALG on external interfaces. **Checked** - the SIP ALG will be switched off. **Unchecked** - the SIP ALG will not work.
Device Metric	Value of Metric of IP network on this interface in the Routing Table. Range is 0-255, with a default of 20.
Default Route	Check to enable default route. Default is enabled.
Routing Protocol	**None -** Disable the routing protocol on this interface. **OSPF** - Set the routing protocol to OSPF on this interface. There is a link below the option to configure OSPF. **RIP** - Set the routing protocol to RIP on this interface. **Listen to RIP Messages** - None, RIPv1, RIPv2, RIPv1/2 **Send RIP Messages** - None, RIPv1, RIPv2 - Broadcast, RIPv2 - Multicast
Internet Connection Firewall	**Note:** This name is a link to the *Security* window Enables/disables Firewall for this device.
Additional IP Addresses	Opens a window to add an additional IP address with subnet mask.

NOTE: The Adit uses the compressed format of protocol encapsulation, which means it uses a 1-byte protocol instead of 2 bytes. The unit automatically detects when the opposite end does not support this, by protocol rejects, and reverts to uncompressed to accommodate older devices that may not support Rx on the 1-byte format.

Serial (PPPoDS0)

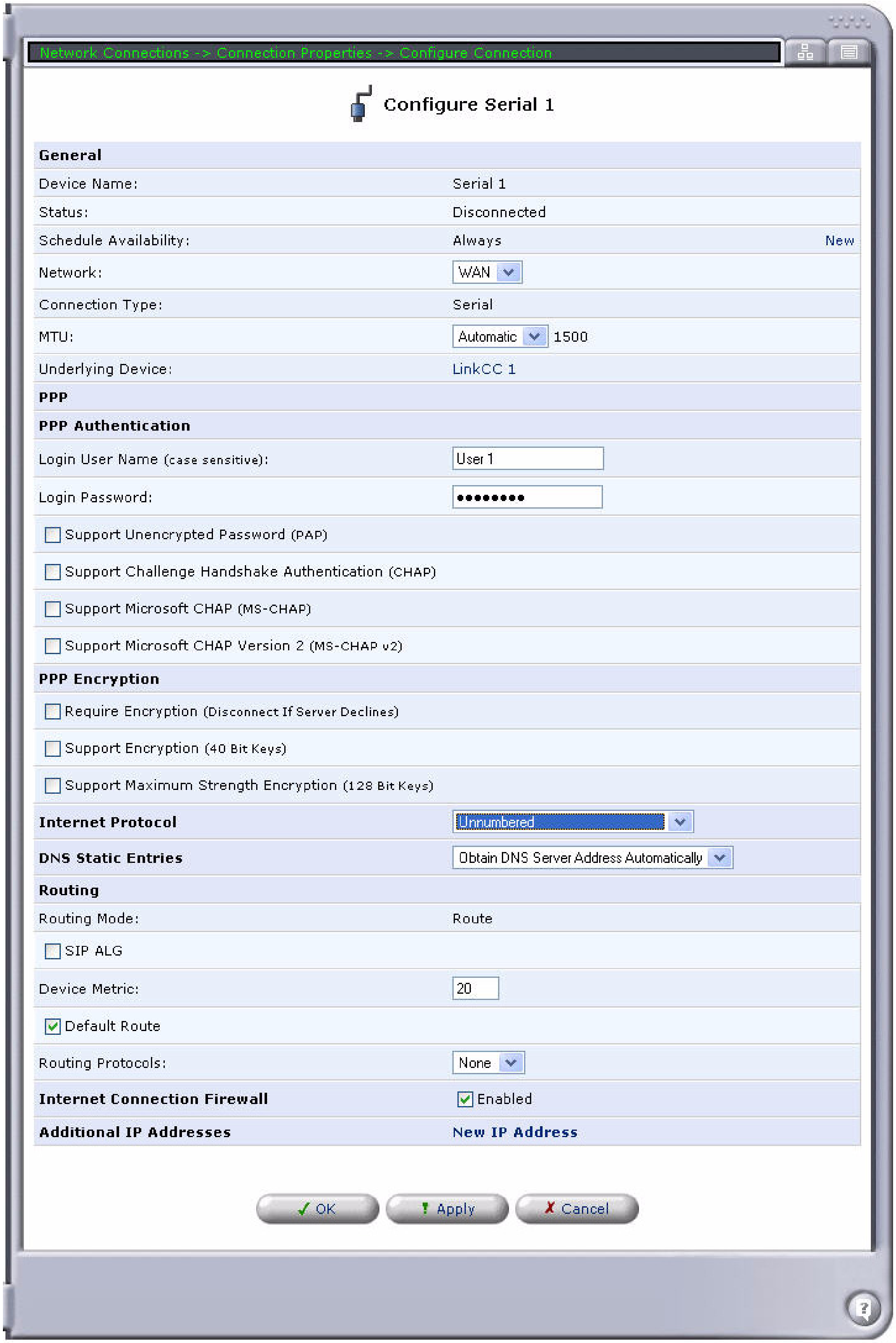
The Serial Properties window displays the settings of a Serial PPP over DS0 connection. For the MSR, this connection must be configured with the **New Connection** option. (See *New Connection* on page 3-27.) For the Adit 3000, Serial 1 is a preconfigure connection. You can select the connection to view its properties, modify its settings, or disable/enable it.

A sample Serial Properties window for the Adit MSR is shown below. Note that the **Underlying Device** is a Link Cross-Connect (LCC). For the Adit 3000, the **Underlying Device** is a T1.



Name:	Serial 1
Device Name:	Serial 1
Status:	Disconnected
Network:	WAN
Underlying Device:	LinkCC 1
Connection Type:	Serial
IP Address:	Unnumbered
Subnet Mask:	
User Name:	User 1
Channel Start:	0
Channel End:	0
Received Packets:	0
Sent Packets:	0

If necessary, you can modify the serial connection by selecting the **Settings** button. The **Configure Serial 1** window appears, as shown in the following figure.



Network Connections -> Connection Properties -> Configure Connection

Configure Serial 1

General		
Device Name:	Serial 1	
Status:	Disconnected	
Schedule Availability:	Always	New
Network:	WAN	
Connection Type:	Serial	
MTU:	Automatic 1500	
Underlying Device:	LinkCC 1	
PPP		
PPP Authentication		
Login User Name (case sensitive):	User 1	
Login Password:	••••••••	
□ Support Unencrypted Password (PAP)		
□ Support Challenge Handshake Authentication (CHAP)		
□ Support Microsoft CHAP (MS-CHAP)		
□ Support Microsoft CHAP Version 2 (MS-CHAP v2)		
PPP Encryption		
□ Require Encryption (Disconnect If Server Declines)		
□ Support Encryption (40 Bit Keys)		
□ Support Maximum Strength Encryption (128 Bit Keys)		
Internet Protocol	Unnumbered	
DNS Static Entries	Obtain DNS Server Address Automatically	
Routing		
Routing Mode:	Route	
□ SIP ALG		
Device Metric:	20	
☑ Default Route		
Routing Protocols:	None	
Internet Connection Firewall	☑ Enabled	
Additional IP Addresses	New IP Address	

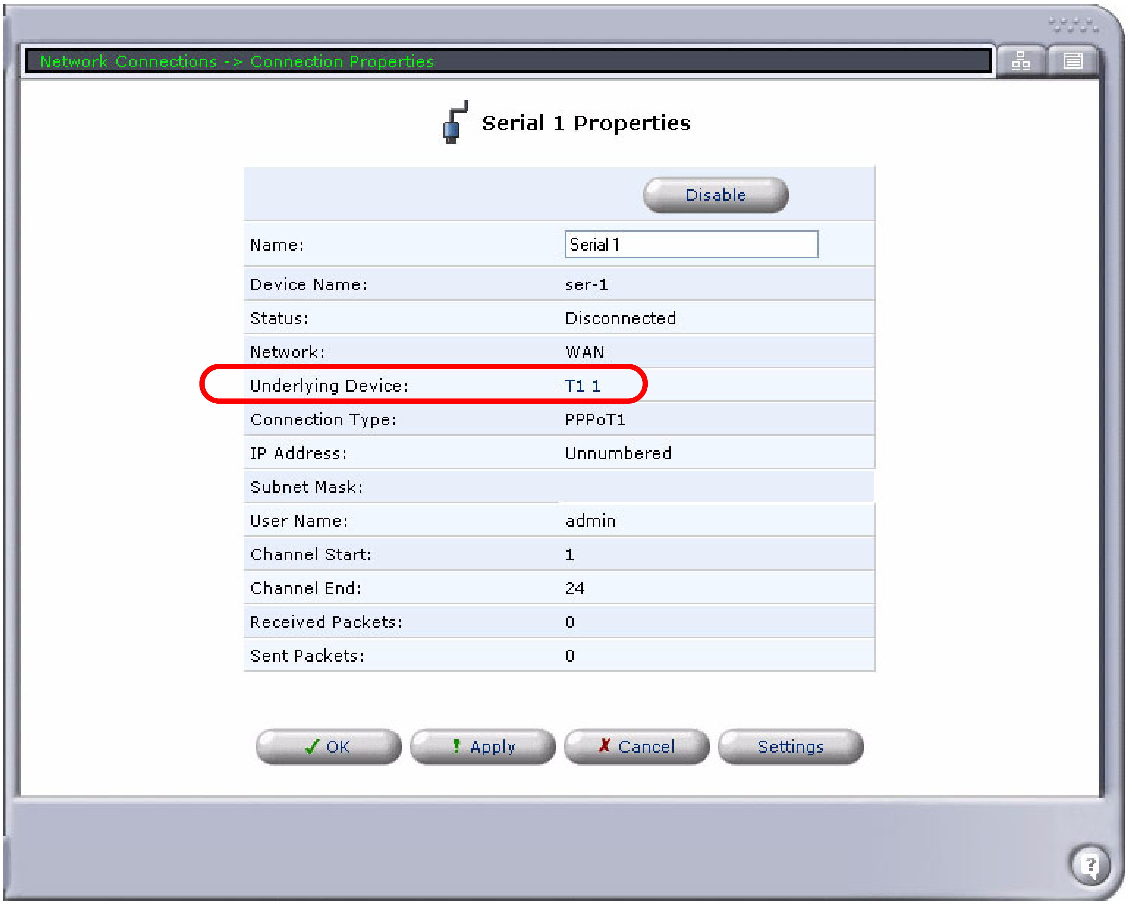
The following are field definitions for the **Configure Serial 1** window:

Field	Definition
General	
Device Name	Displays the device name.
Status	Displays the current status.
Schedule Availability	Defines when the WAN is available. The default is **Always**. To create a Schedule Availability rule, click **New**.
Network	Defines the type of network: **WAN** - Wide Area Network (Default). **LAN** - Local Area Network **DMZ** - Demilitarized Zone
Connection Type	Displays the connection type: **Adit 3000:** PPPoT1 **Adit MSR:** Serial
MTU	Maximum Transmission Unit. Sets the largest packet size (bytes) the network will transmit. **Automatic** at 1500 **Manual** at a range of 576 to 1500.
Underlying Device	Displays the device/connection required for this interface: **Adit 3000:** Displays the T1 in this connection. This is a link to the High Speed Serial Configuration window. See *Underlying Device - High Speed Serial Configuration (Adit 3000 Only)* on page 3-25. **Adit MSR:** Displays the LCC in this connection.
PPP - Note: These fields do not display when The Internet Protocol field is set to "unnumbered"	
On Demand	Attempts to connect only when packets are sent.
Time Between Reconnect Attempt	Sets the interval of time between reconnect attempts. Range is 0 - 99999 seconds. Default is 30 seconds.
Restart Timer	Range is 1 - 65535 seconds. Default is 3 seconds.
PPP Authentication	
Login User Name	Enter Login User Name, with a maximum of 100 characters.
Login Password	Enter login password. Select to enable support of the following: **Support Unencrypted Password (PAP)** **Support Challenge Handshake Authentication (CHAP)** **Support Microsoft CHAP (MS-CHAP)** **Support Microsoft CHAP Version 2 (MS-CHAPv2)**
PPP Encryption	The following PPP encryption can be enabled by checking the boxes: **Require Encryption** (Disconnect if server declines) **Support Encryption** (40 bit keys) **Support Maximum Strength Encryption** (128 bit keys)
Internet Protocol	
Unnumbered	Treat this as an un-numbered interface per RFC 1812. Default.
Obtain an IP Address Automatically	Sets the WAN to use DHCP to obtain an IP address. **Override Subnet Mask** - Set mask, override any previous setting.
Use the Following IP Address	**IP Address** - Sets the IP Address **Override Subnet Mask** - Set mask, override any previous setting.

Field	Definition (Continued)
DNS Static Entries (This name is a link to the *Advanced/DNS Static Entries* window.)	
Obtain DNS Server Address Automatically	Sets the interface to obtain a DNS Server address.
Use the Following DNS Server Address	Sets the DNS Server Address. **Primary DNS Server** - Enter the specific DNS server address to use. **Secondary DNS Server** - Enter a secondary DNS server address to use.
Routing	
Routing Mode	Displays the current routing mode. **Route -** Routing is used if public is visible on both sides. **NAPT -** NAPT is used if doing private IPs on the Ethernet side or if you want to hide specific publics on the internal side.
SIP ALG	This field allows the customer to turn off the SIP ALG on external interfaces. **Checked** - the SIP ALG will be switched off. **Unchecked** - the SIP ALG will not work.
Device Metric	Value of Metric of IP network on this interface in the Routing Table. Range is 0-255, with a default of 20.
Default Route	Check to enable default route.
Routing Protocol	**None -** Disable the routing protocol on this interface. **OSPF** - Set the routing protocol to OSPF on this interface. There is a link below the option to configure OSPF. **RIP** - Set the routing protocol to RIP on this interface. **Listen to RIP Messages** - None, RIPv1, RIPv2, RIPv1/2 **Send RIP Messages** - None, RIPv1, RIPv2 - Broadcast, RIPv2 - Multicast
Internet Connection Firewall	**Note:** This name is a link to the *Security* window Enables/Disables Firewall for this device.
Additional IP Addresses	Opens a window to add an additional IP address with subnet mask.

Underlying Device - High Speed Serial Configuration (Adit 3000 Only)

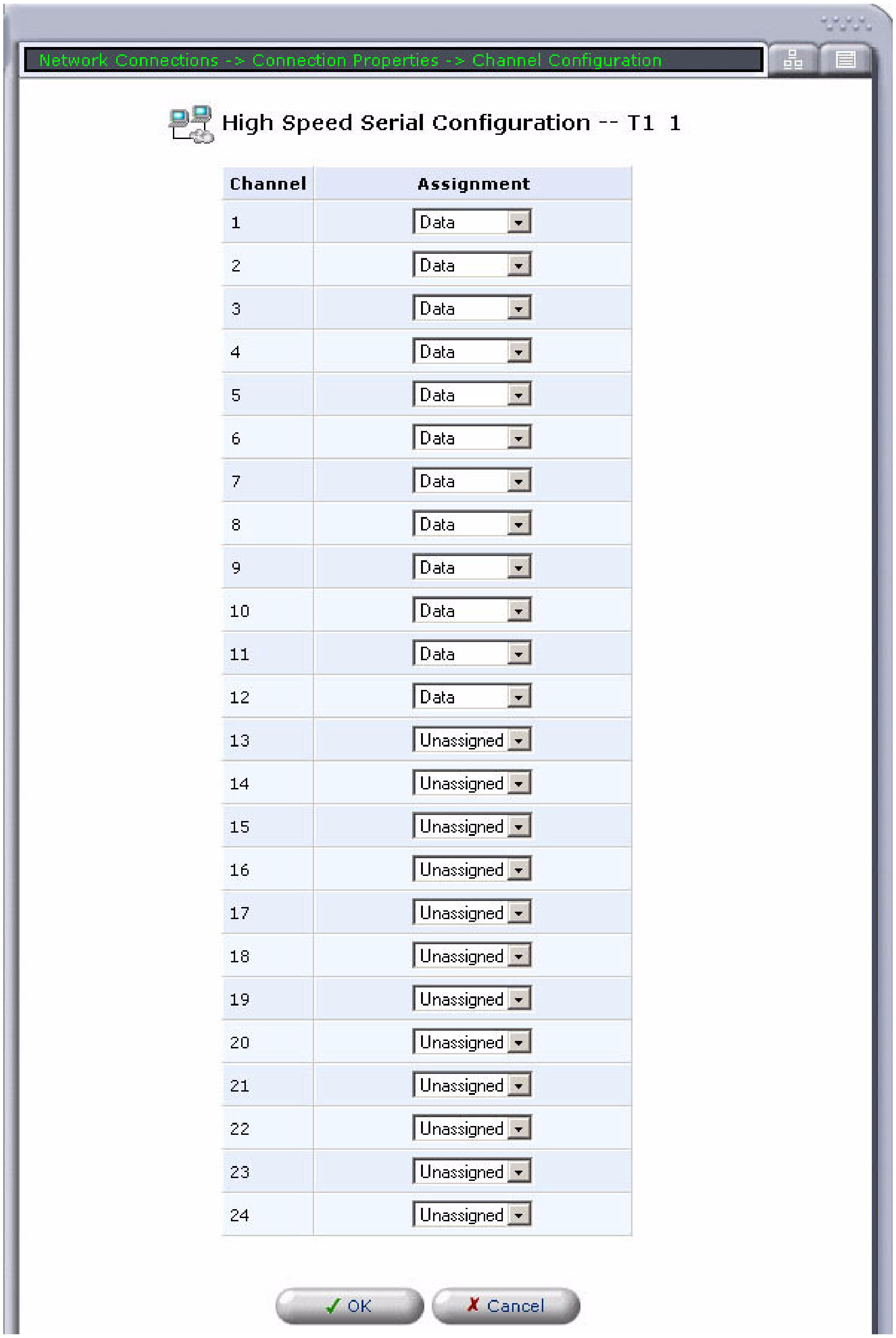
To configure the individual channels in the Serial 1 (PPPoT1) or Multilink connection, select the **T1** name listed in the **Underlying Device** field.



Serial 1 Properties

Name:	Serial 1
Device Name:	ser-1
Status:	Disconnected
Network:	WAN
Underlying Device:	T1 1
Connection Type:	PPPoT1
IP Address:	Unnumbered
Subnet Mask:	
User Name:	admin
Channel Start:	1
Channel End:	24
Received Packets:	0
Sent Packets:	0

The High Speed Serial Configuration window is shown on the following page. Use this window to set the channel assignments.



Network Connections -> Connection Properties -> Channel Configuration

High Speed Serial Configuration -- T1 1

Channel	Assignment
1	Data
2	Data
3	Data
4	Data
5	Data
6	Data
7	Data
8	Data
9	Data
10	Data
11	Data
12	Data
13	Unassigned
14	Unassigned
15	Unassigned
16	Unassigned
17	Unassigned
18	Unassigned
19	Unassigned
20	Unassigned
21	Unassigned
22	Unassigned
23	Unassigned
24	Unassigned

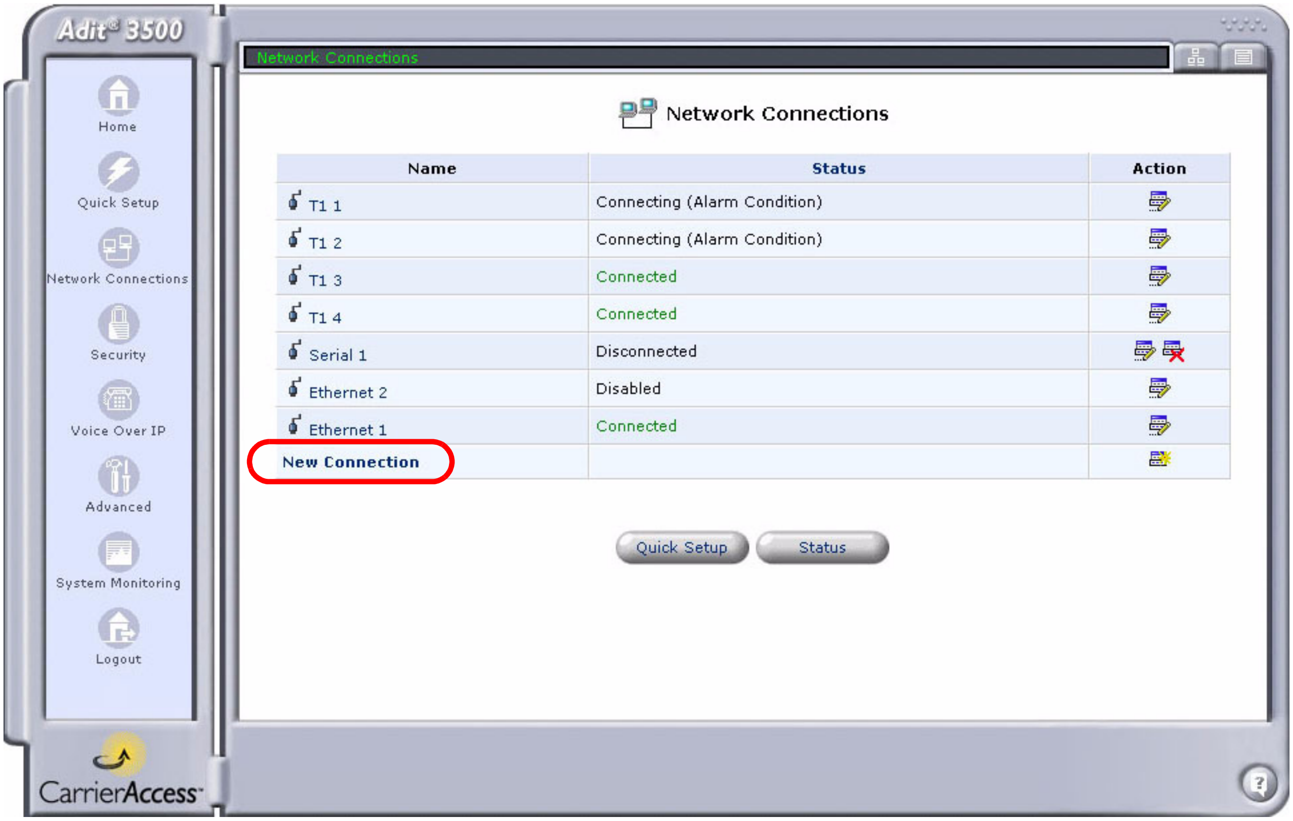
Field	Definition
Assignment	**Data** - Sets the channel type to Data. **Unassigned** - Puts the channel out-of-service (down). Default.

New Connection

There are a variety of options for creating a **New Connection**. The following sections walk through each option.

- **Point-to-Point Protocol over DS0 (Serial)**
- **Multilink Point-to-Point Protocol over DS0 (Multilink)**
- **Point-to-Point Tunneling Protocol (PPTP)**
- **Point-to-Point Tunneling Protocol Server (PPTP Server)**
- **Layer Two Tunneling Protocol (L2TP)**
- **Internet Protocol Security (IPSec)**

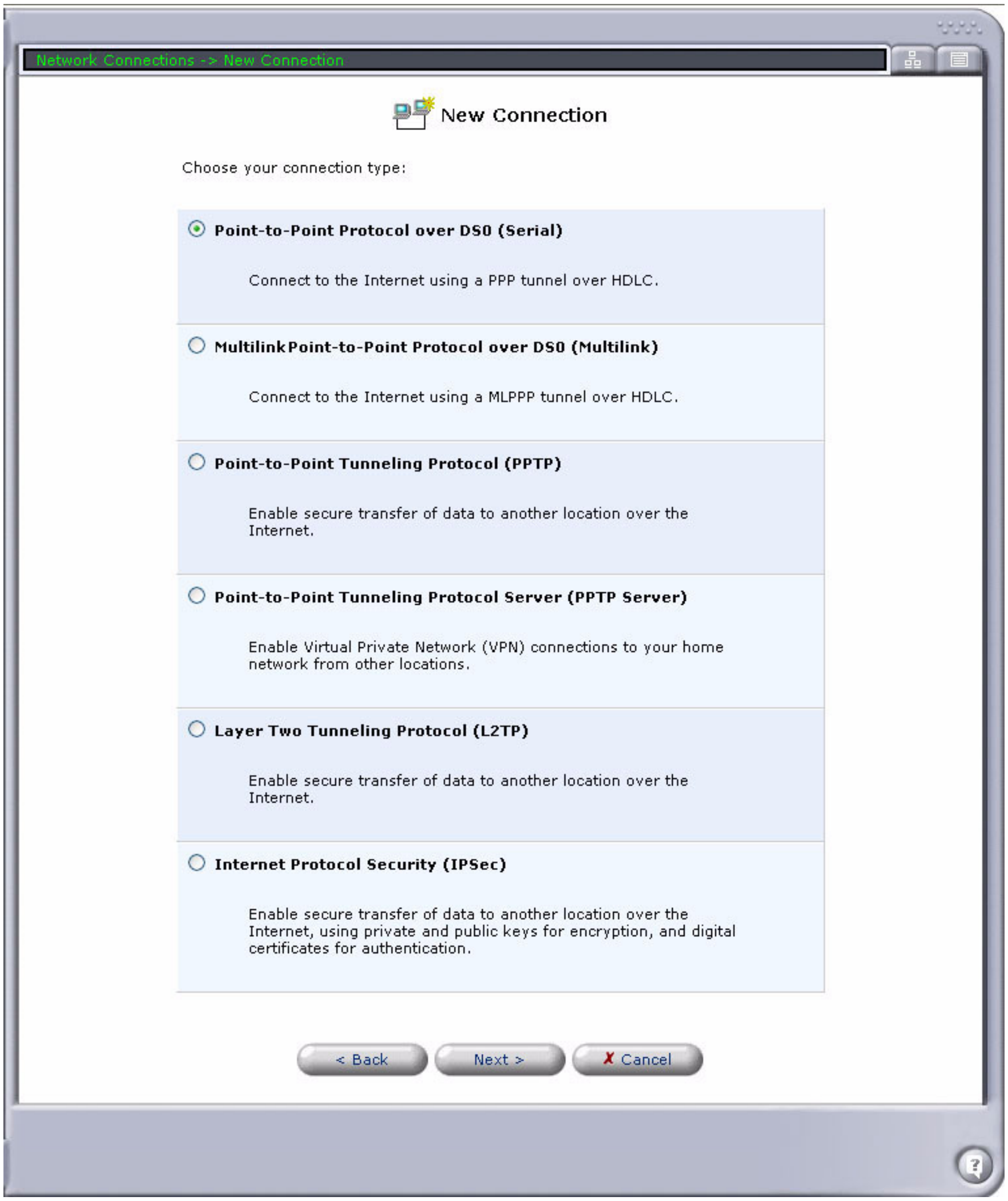
NOTE: For information on modifying these connections after setup, see *Connections that Require Configuration* on page 3-16.



Network Connections

Name	Status	Action
T1 1	Connecting (Alarm Condition)	
T1 2	Connecting (Alarm Condition)	
T1 3	Connected	
T1 4	Connected	
Serial 1	Disconnected	
Ethernet 2	Disabled	
Ethernet 1	Connected	
New Connection		

New Connection Window



New Connection

Choose your connection type:

● **Point-to-Point Protocol over DS0 (Serial)**

Connect to the Internet using a PPP tunnel over HDLC.

○ **MultilinkPoint-to-Point Protocol over DS0 (Multilink)**

Connect to the Internet using a MLPPP tunnel over HDLC.

○ **Point-to-Point Tunneling Protocol (PPTP)**

Enable secure transfer of data to another location over the Internet.

○ **Point-to-Point Tunneling Protocol Server (PPTP Server)**

Enable Virtual Private Network (VPN) connections to your home network from other locations.

○ **Layer Two Tunneling Protocol (L2TP)**

Enable secure transfer of data to another location over the Internet.

○ **Internet Protocol Security (IPSec)**

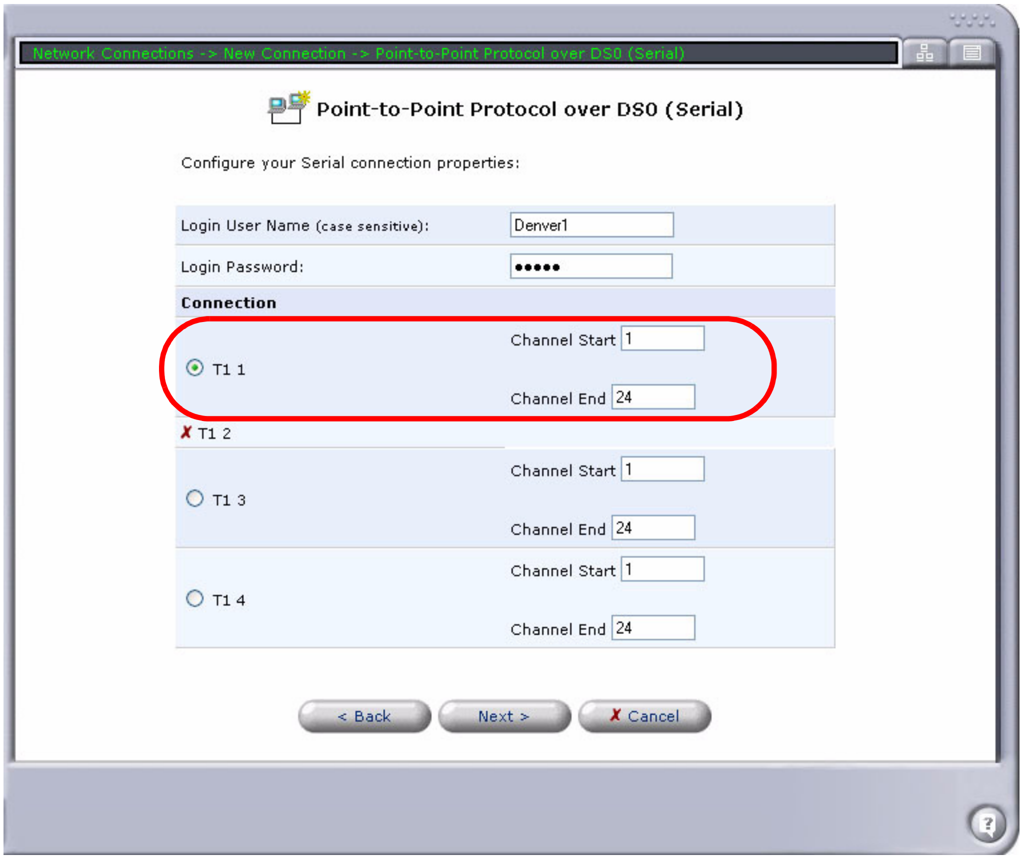
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption, and digital certificates for authentication.

Point-to-Point Protocol over DS0 (Serial)

PPPoDS0 (Serial) creates a connection to the Internet using a PPP tunnel over HDLC. This configuration creates a **Serial 1** connection listed on the Network Connections table. This connection can be enabled, disabled, modified, and deleted.

NOTE: For the Adit MSR, cross-connects from Adit 600 resources (T1 lines or WAN-capable cards) must be made before setting up the WAN link. All DS0s cross-connected to the WAN link must be of type "Data." Use the **connect (msr)** command from the Adit 600 controller to cross-connect resources to the MSR card. See the *Adit 600 User Manual* for more information.

1. Select **Network Connections/New Connection.**
2. Select **Point-to-Point Protocol over DS0 (Serial)**, then select **Next** >.
3. Add a Login **User Name** and **Password** for this Serial connection.
4. Select the **Connection** to be used for this WAN:
   - **Adit 3000:** Select the T1 and specify the channel range for the T1.
   - **Adit MSR:** Select the LCC.



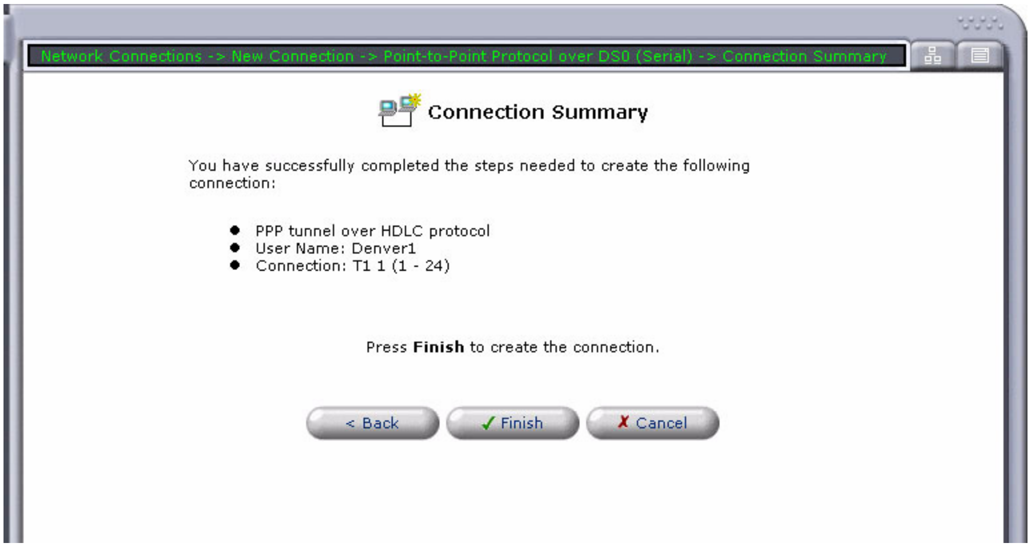
Network Connections -> New Connection -> Point-to-Point Protocol over DS0 (Serial)

Point-to-Point Protocol over DS0 (Serial)

Configure your Serial connection properties:

Login User Name (case sensitive):	Denver1
Login Password:	●●●●●
Connection	
● T1 1	Channel Start 1 Channel End 24
✗ T1 2	
○ T1 3	Channel Start 1 Channel End 24
○ T1 4	Channel Start 1 Channel End 24

5. Select **Next >**.



Network Connections -> New Connection -> Point-to-Point Protocol over DS0 (Serial) -> Connection Summary

Connection Summary

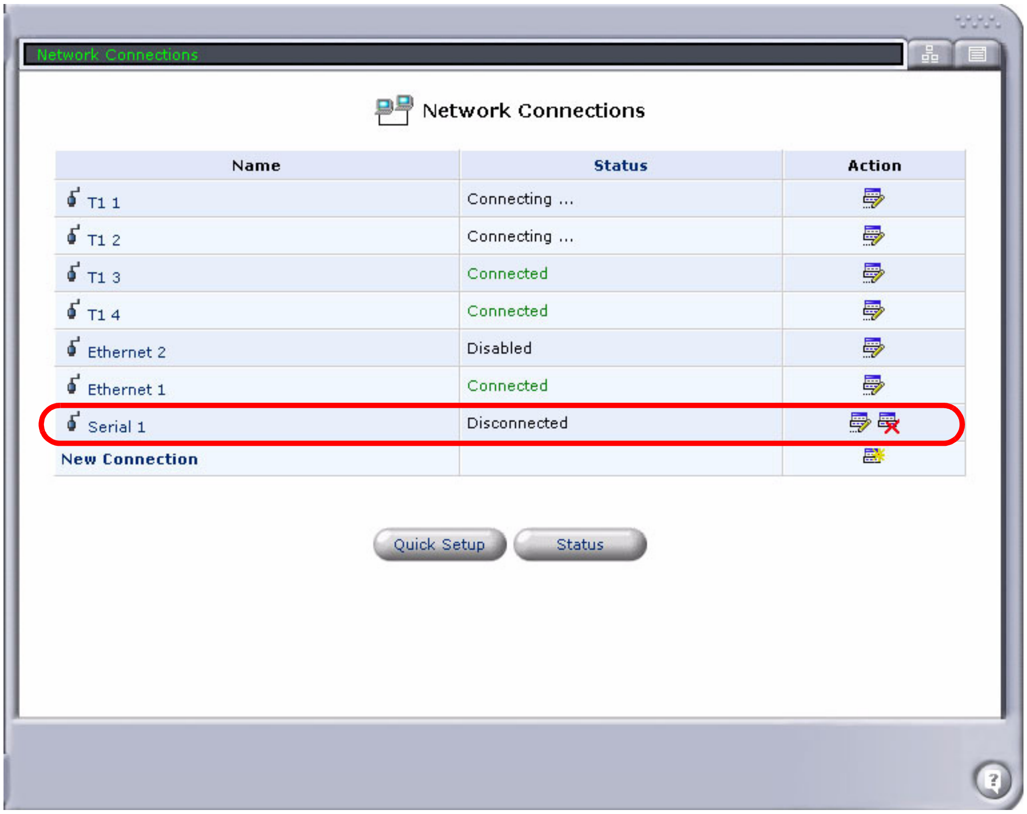
You have successfully completed the steps needed to create the following connection:

- PPP tunnel over HDLC protocol
- User Name: Denver1
- Connection: T1 1 (1 - 24)

Press **Finish** to create the connection.

6. The Connection Summary window displays the current configuration.
Select ✓**Finish** if information is correct.
Select < **Back** to modify the configuration.
Select ✗ **Cancel** to stop this setup and return to the Network Connections window.

7. The new Serial connection appears on the Network Connections window.



Network Connections

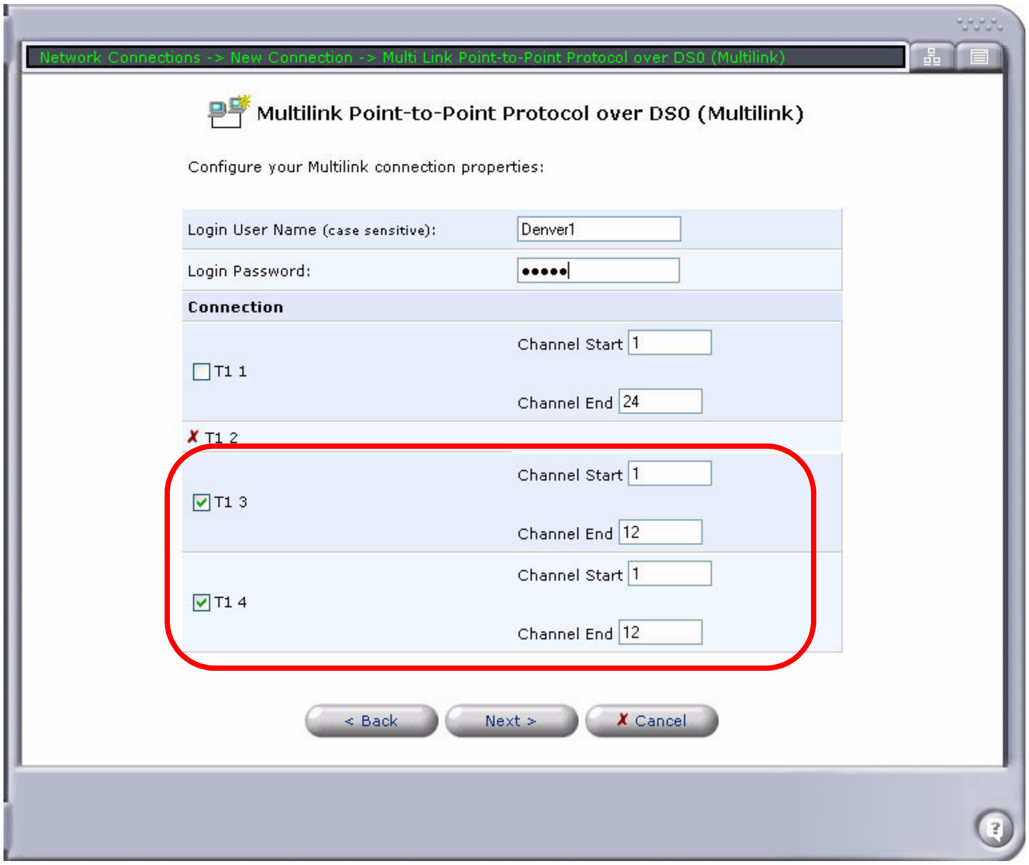
Name	Status	Action
T1 1	Connecting ...	
T1 2	Connecting ...	
T1 3	Connected	
T1 4	Connected	
Ethernet 2	Disabled	
Ethernet 1	Connected	
Serial 1	Disconnected	
New Connection		

Multilink Point-to-Point Protocol over DS0 (Multilink)

Multilink creates a connection to the Internet using a MLPPP tunnel over HDLC. This configuration creates a **Multilink 1** connection listed on the Network Connections table. This connection can be enabled, disabled, modified, and deleted.

NOTE: For the Adit MSR, cross-connects from Adit 600 resources (T1 lines or WAN-capable cards) must be made before setting up the WAN link. All DS0s cross-connected to the WAN link must be of type "Data." Use the **connect (msr)** command from the Adit 600 controller to cross-connect resources to the MSR card. See the *Adit 600 User Manual* for more information.

1. Select **Network Connections/New Connection.**
2. Select **Multilink Point-to-Point Protocol over DS0 (Multilink)**, then select **Next** >.
3. Add a Login **User Name** and **Password** for this Multilink connection.
4. Select the **Connections** to be used for this WAN:
   - **Adit 3000:** Select the T1s and specify the channel range for each T1.
   - **Adit MSR:** Select the LCCs.



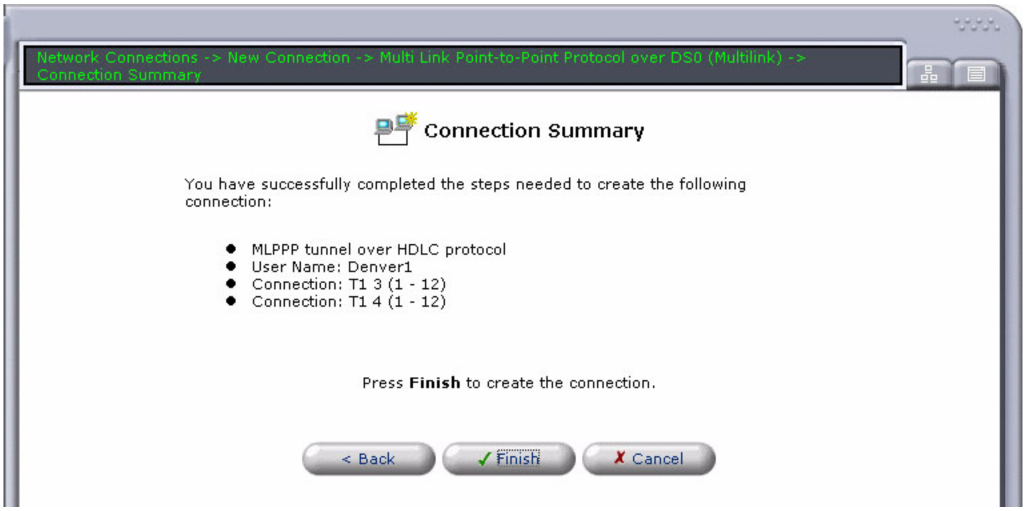
Network Connections -> New Connection -> Multi Link Point-to-Point Protocol over DS0 (Multilink)

Multilink Point-to-Point Protocol over DS0 (Multilink)

Configure your Multilink connection properties:

Login User Name (case sensitive):	Denver1
Login Password:	•••••
Connection	
□ T1 1	Channel Start 1 Channel End 24
✗ T1 2	
☑ T1 3	Channel Start 1 Channel End 12
☑ T1 4	Channel Start 1 Channel End 12

5. Select **Next >**.



Network Connections -> New Connection -> Multi Link Point-to-Point Protocol over DS0 (Multilink) -> Connection Summary

Connection Summary

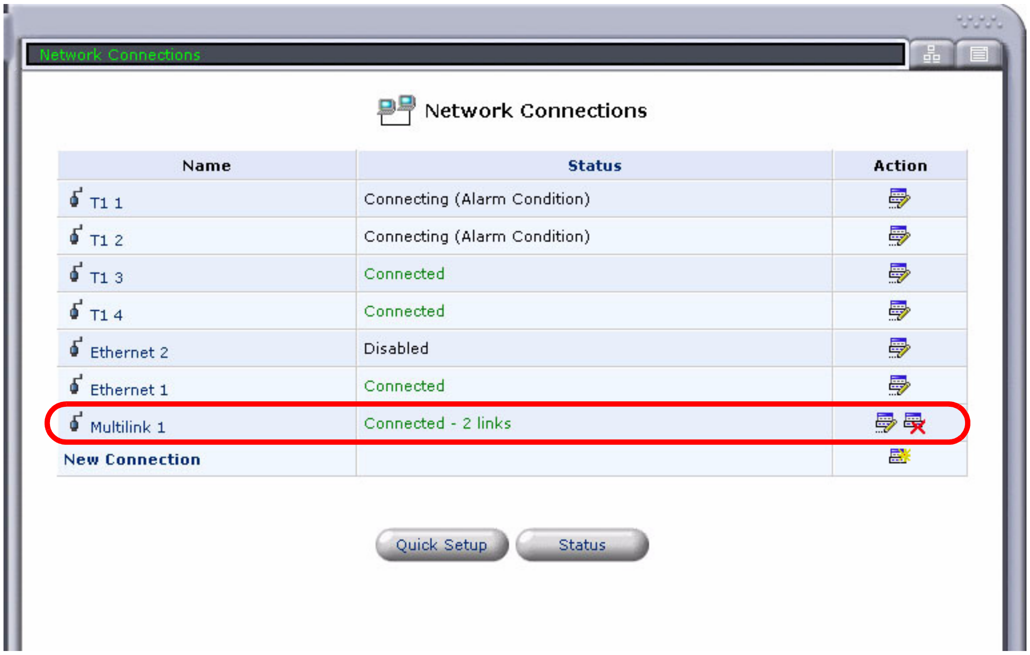
You have successfully completed the steps needed to create the following connection:

- MLPPP tunnel over HDLC protocol
- User Name: Denver1
- Connection: T1 3 (1 - 12)
- Connection: T1 4 (1 - 12)

Press **Finish** to create the connection.

6. The Connection Summary window displays the current configuration.
Select ✓ **Finish** if information is correct.
Select < **Back** to modify the configuration.
Select ✗ **Cancel** to stop this setup and return to the Network Connections window.

7. The new Multilink connection appears on the Network Connections window.



Network Connections

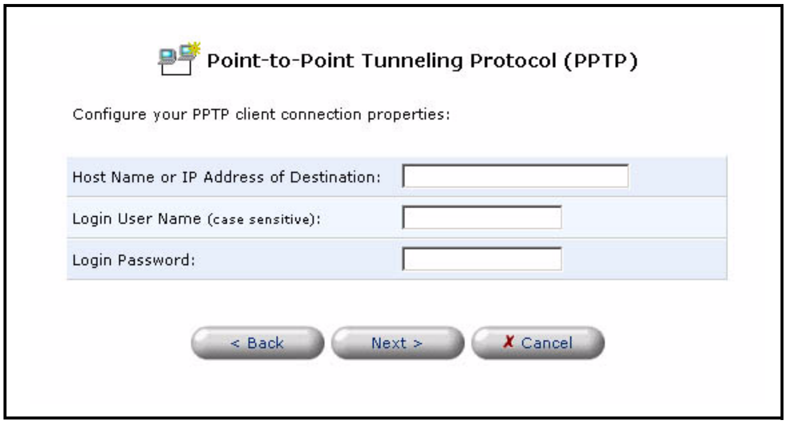
Network Connections

Name	Status	Action
T1 1	Connecting (Alarm Condition)	
T1 2	Connecting (Alarm Condition)	
T1 3	Connected	
T1 4	Connected	
Ethernet 2	Disabled	
Ethernet 1	Connected	
Multilink 1	Connected - 2 links	
New Connection		

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol enables secure transfer of data to another location over the Internet.

1. Select **Network Connections/New Connection**.
2. Select **Point-to-Point Tunneling Protocol (PPTP)**, then select **Next >**.



Point-to-Point Tunneling Protocol (PPTP)

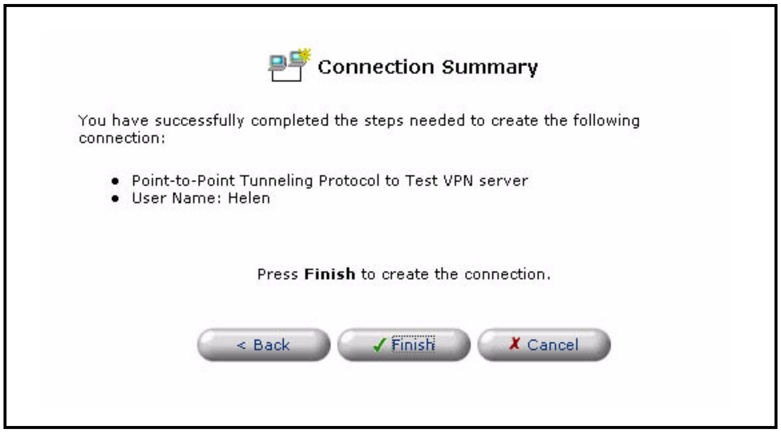
Configure your PPTP client connection properties:

Host Name or IP Address of Destination:	
Login User Name (case sensitive):	
Login Password:	

3. Configure the Client Connection Properties:

Field	Definition
Host Name or IP Address of Destination	Enter the Remote Server Host Name or IP Address.
Login User Name	Enter the User Name for the above server.
Login Password	Enter the Password for the above User Name.

4. Select **Next >**.



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol to Test VPN server
- User Name: Helen

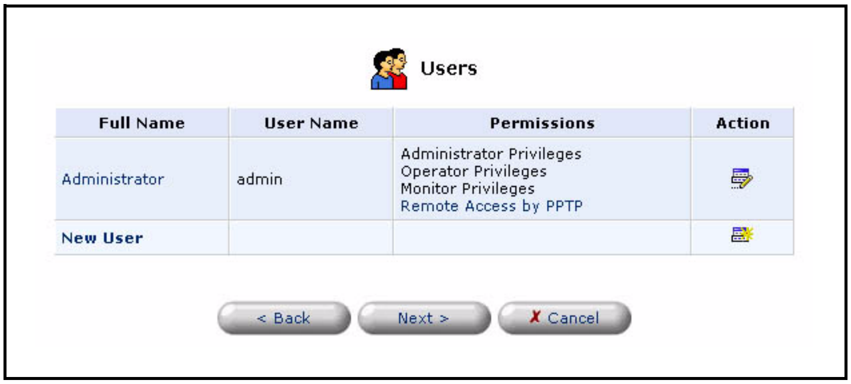
Press **Finish** to create the connection.

5. Select ✓**Finish**.

Point-to-Point Tunneling Protocol Server (PPTP Server)

PPTP Server enables Virtual Private Network (VPN) connections to your home network from other locations.

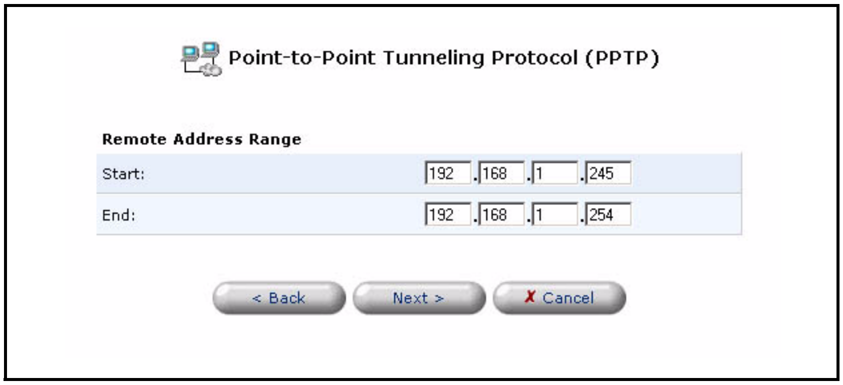
1. Select **Network Connections/New Connection**.
2. Select **Point-to-Point Tunneling Protocol Server (PPTP Server)**, then select **Next >**.



Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator Privileges Operator Privileges Monitor Privileges Remote Access by PPTP	
New User			

3. Add a User by selecting **New User**. See *Adding a User* on page 2-66 for more information.
4. Select **Next >**.



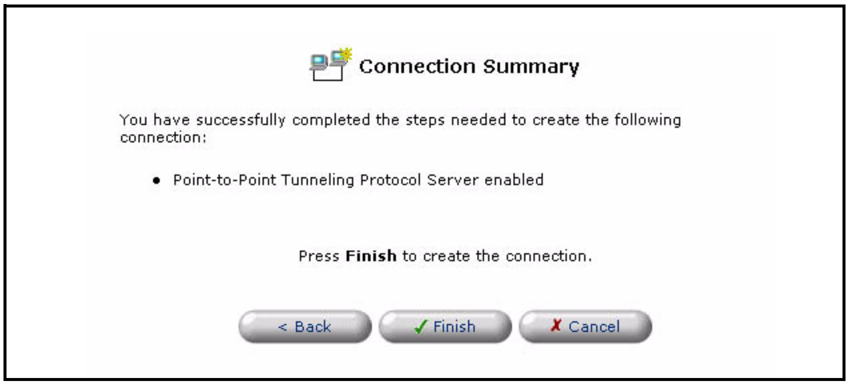
Point-to-Point Tunneling Protocol (PPTP)

Remote Address Range

Start:	192 . 168 . 1 . 245
End:	192 . 168 . 1 . 254

5. The **Start** and **End** Remote Address Range are automatically supplied. Modify the addresses, if needed.

6. Select **Next >**.



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol Server enabled

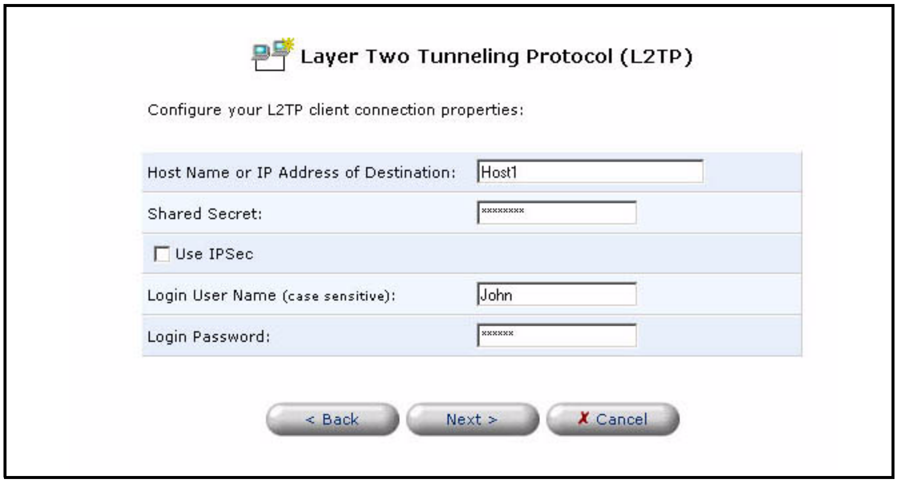
Press **Finish** to create the connection.

7. Select ✓**Finish**.

Layer Two Tunneling Protocol (L2TP)

L2TP enables secure transfer of data to another location over the Internet.

1. Select **Network Connections/New Connection.**
2. Select **Layer Two Tunneling Protocol (L2TP)**, then select **Next** >.



Layer Two Tunneling Protocol (L2TP)

Configure your L2TP client connection properties:

Host Name or IP Address of Destination: Host1

Shared Secret: ********

□ Use IPSec

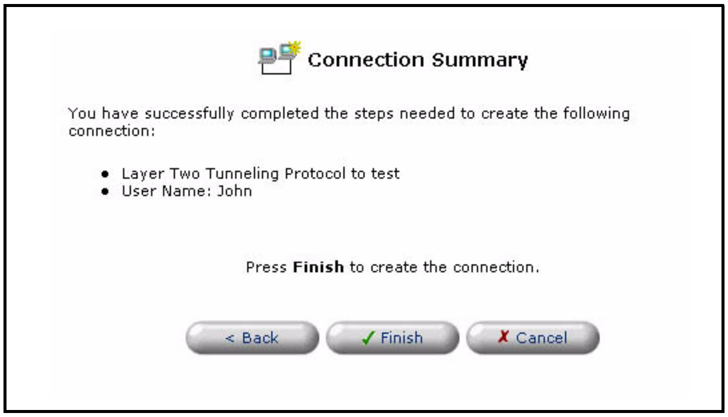
Login User Name (case sensitive): John

Login Password: ******

3. Configure the L2TP client connection properties:

Field	Definition
Host Name or IP Address of Destination	Enter the Remote Server Host Name or IP Address.
Shared Secret	Enter a shared secret key, with a maximum of 30 characters.
Use IPSec	Checkbox enables Internet Protocol Security.
Login User Name	Enter the User Name for the above server.
Login Password	Enter the Password for the above User Name.

4. Select **Next** >.



Connection Summary

You have successfully completed the steps needed to create the following connection:

- Layer Two Tunneling Protocol to test
- User Name: John

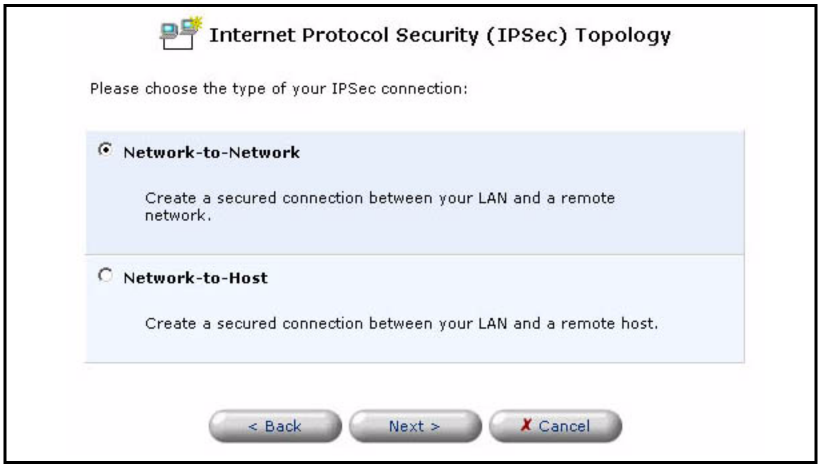
Press **Finish** to create the connection.

5. Select ✓**Finish**.

Internet Protocol Security (IPSec)

IPSec enables secure transfer of data to another location over the Internet, using private and public keys for encryption, and digital certificates for authentication.

1. Select **Network Connections/New Connection.**
2. Select **Internet Protocol Security (IPSec)**, then select **Next >**.
   Note: There are multiple options at each window. The displays vary depending on selections made on the previous window.



Internet Protocol Security (IPSec) Topology

Please choose the type of your IPSec connection:

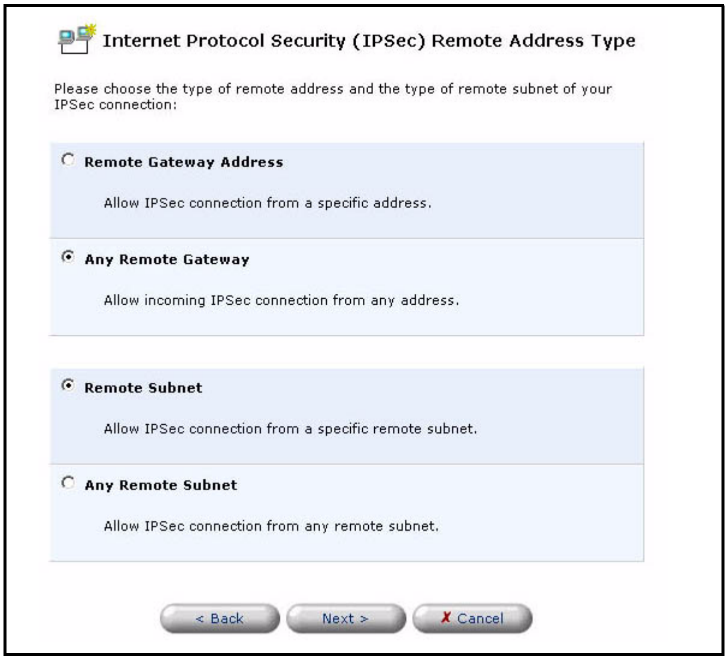
● **Network-to-Network**

Create a secured connection between your LAN and a remote network.

○ **Network-to-Host**

Create a secured connection between your LAN and a remote host.

3. Select the type of IPSec connection (**Network-to-Network** or **Network-to-Host**), and select **Next >**.
   Note: The following example assumes a selection of **Network-to-Network**. There are more options on this window than with the **Network-to-Host** selection.



Internet Protocol Security (IPSec) Remote Address Type

Please choose the type of remote address and the type of remote subnet of your IPSec connection:

○ **Remote Gateway Address**

Allow IPSec connection from a specific address.

● **Any Remote Gateway**

Allow incoming IPSec connection from any address.

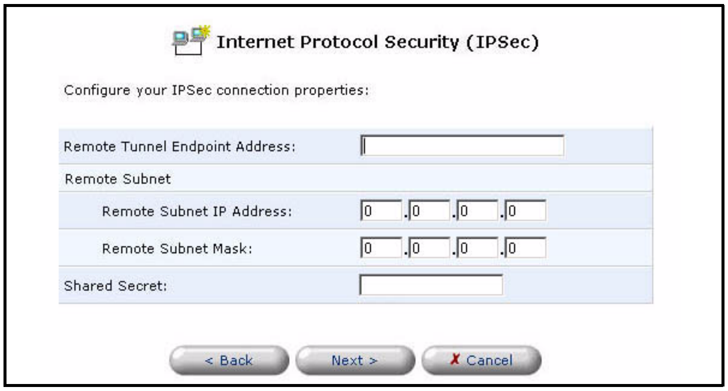
● **Remote Subnet**

Allow IPSec connection from a specific remote subnet.

○ **Any Remote Subnet**

Allow IPSec connection from any remote subnet.

4. Select the Remote Address and Subnet types, and select **Next >**.
   Note: The following example assumes a selection of **Network-to-Network/Remote Gateway Address** and **Remote Subnet**. This example displays the most options.



Internet Protocol Security (IPSec)

Configure your IPSec connection properties:

Remote Tunnel Endpoint Address:

Remote Subnet

Remote Subnet IP Address: 0 .0 .0 .0

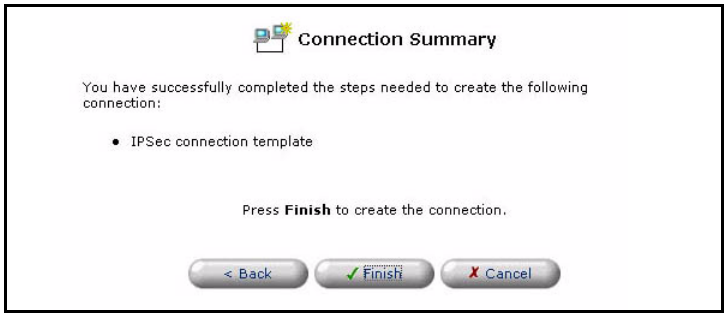
Remote Subnet Mask: 0 .0 .0 .0

Shared Secret:

5. Configure the IPSec connection properties:

Field	Definition
Remote Tunnel Endpoint Address	Enter the Remote Server IP Address.
Remote Subnet	**Remote Subnet IP Address** - Enter the remote subnet IP Address **Remote Subnet Mask** - Enter the subnet mask for the above subnet address.
Shared Secret	Enter a shared secret key, with a maximum of 30 characters.

6. Select **Next >**.



Connection Summary

You have successfully completed the steps needed to create the following connection:

- IPSec connection template

Press **Finish** to create the connection.

7. Select ✓**Finish**.

OSPF Configuration on the Network Connection

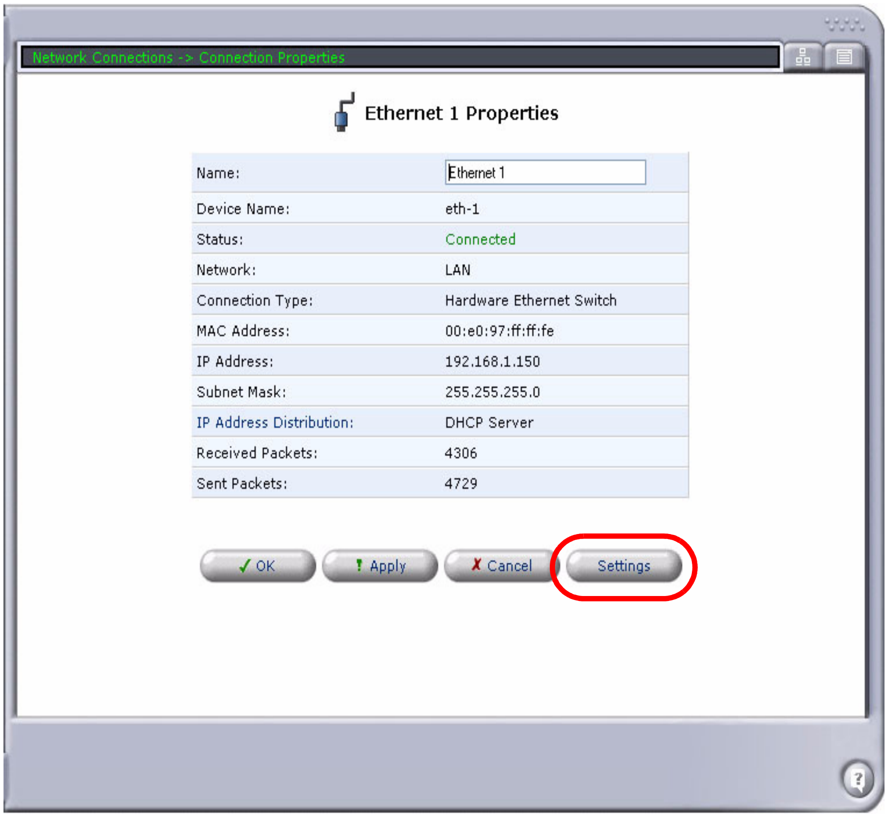
OSPF can be set as the routing protocol on the following network connections:

- Ethernet 1
- Ethernet 2
- Serial
- Multilink

NOTE: The following example uses the Ethernet 1 network connection. Configuration is the same for the Ethernet 2, Serial 1, and Multilink connections.

To configure OSPF on a network connection:

1. Select **Network Connections**, and select the **Ethernet 1** connection name to open the Ethernet 1 Properties window.



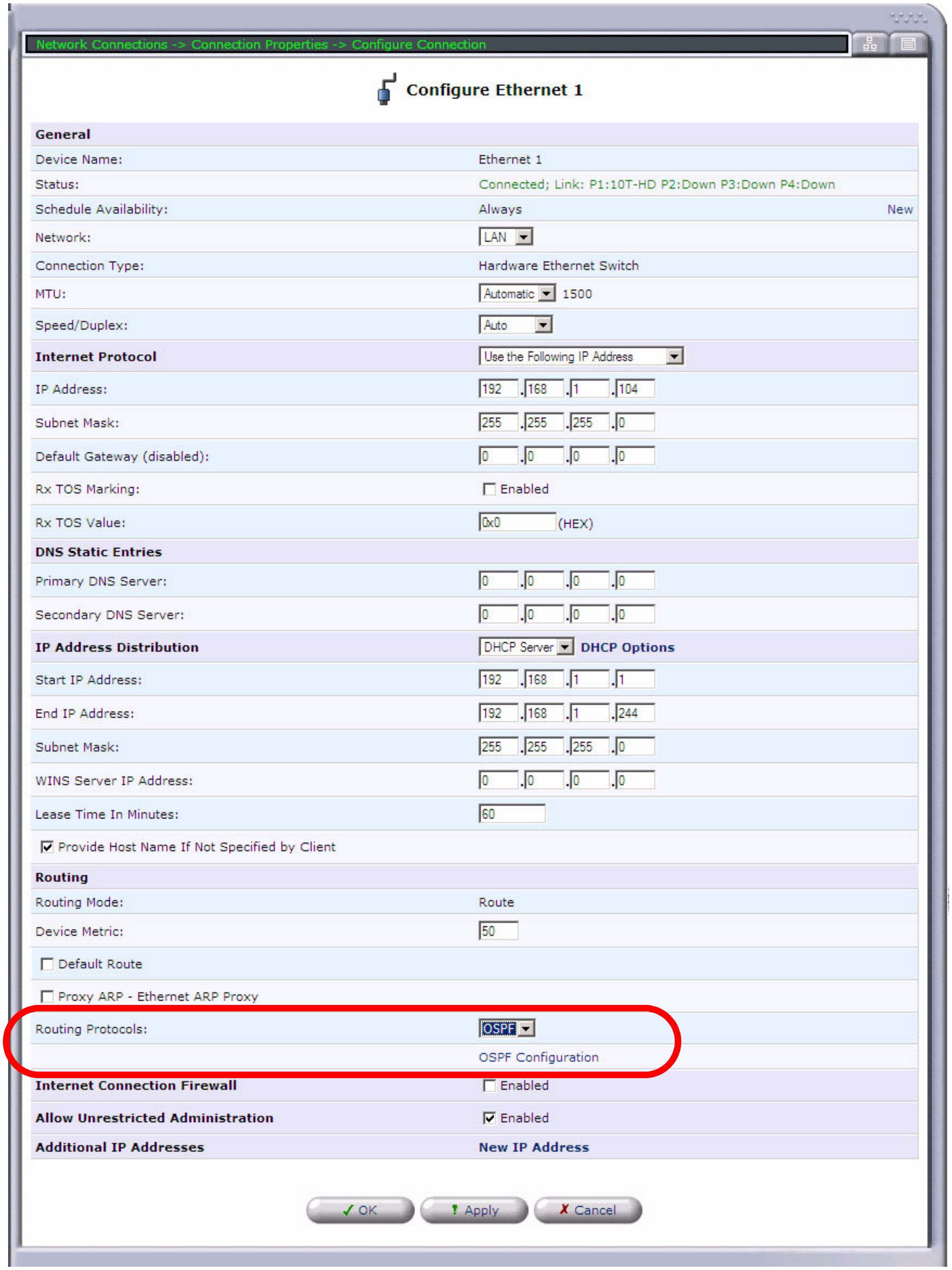
Network Connections -> Connection Properties

Ethernet 1 Properties

Name:	Ethernet 1
Device Name:	eth-1
Status:	Connected
Network:	LAN
Connection Type:	Hardware Ethernet Switch
MAC Address:	00:e0:97:ff:ff:fe
IP Address:	192.168.1.150
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Received Packets:	4306
Sent Packets:	4729

2. Select the **Settings** button.

3. At the Configure Ethernet 1 window, select **OSPF** from the **Routing Protocols** pulldown menu. Click on the **OSPF Configuration** link under the pulldown menu.

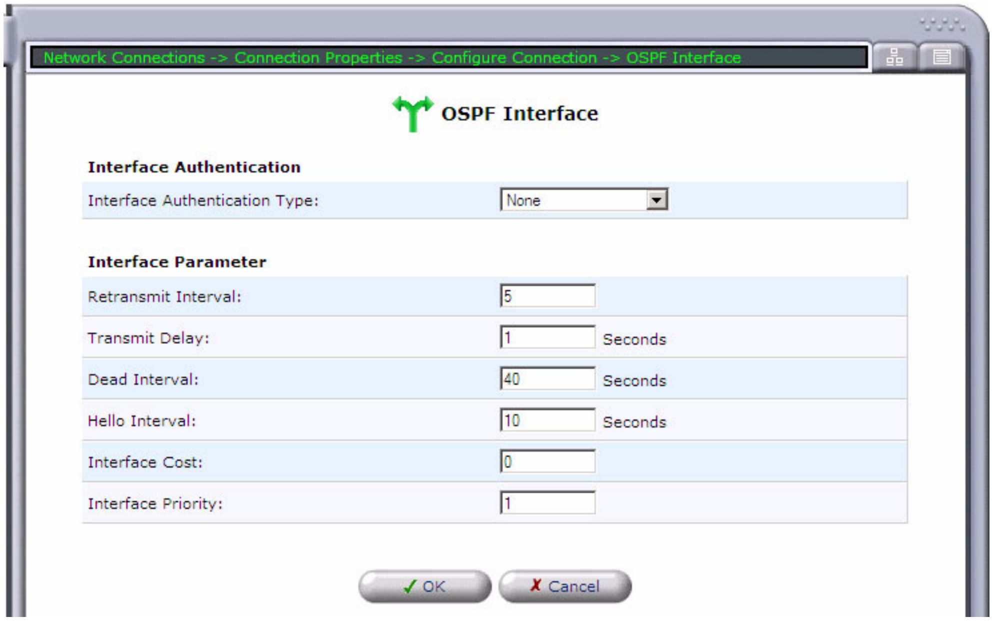


Network Connections -> Connection Properties -> Configure Connection

Configure Ethernet 1

General	
Device Name:	Ethernet 1
Status:	Connected; Link: P1:10T-HD P2:Down P3:Down P4:Down
Schedule Availability:	Always New
Network:	LAN
Connection Type:	Hardware Ethernet Switch
MTU:	Automatic 1500
Speed/Duplex:	Auto
Internet Protocol	Use the Following IP Address
IP Address:	192 .168 .1 .104
Subnet Mask:	255 .255 .255 .0
Default Gateway (disabled):	0 .0 .0 .0
Rx TOS Marking:	□ Enabled
Rx TOS Value:	0x0 (HEX)
DNS Static Entries	
Primary DNS Server:	0 .0 .0 .0
Secondary DNS Server:	0 .0 .0 .0
IP Address Distribution	DHCP Server **DHCP Options**
Start IP Address:	192 .168 .1 .1
End IP Address:	192 .168 .1 .244
Subnet Mask:	255 .255 .255 .0
WINS Server IP Address:	0 .0 .0 .0
Lease Time In Minutes:	60
☑ Provide Host Name If Not Specified by Client	
Routing	
Routing Mode:	Route
Device Metric:	50
□ Default Route	
□ Proxy ARP - Ethernet ARP Proxy	
Routing Protocols:	OSPF
	OSPF Configuration
Internet Connection Firewall	□ Enabled
Allow Unrestricted Administration	☑ Enabled
Additional IP Addresses	**New IP Address**

4. Set the OSPF interface parameters as needed:



Network Connections -> Connection Properties -> Configure Connection -> OSPF Interface

OSPF Interface

Interface Authentication

Interface Authentication Type: None

Interface Parameter

Retransmit Interval: 5

Transmit Delay: 1 Seconds

Dead Interval: 40 Seconds

Hello Interval: 10 Seconds

Interface Cost: 0

Interface Priority: 1

Field	Definition
Interface Authentication	
Interface Authentication Type	**None** - Set the OSPF Authentication to none. **Simple Authentication** - Enable Simple Authentication on the OSPF Interface. **Authentication Password -** Enter password with a maximum 8 characters. **Message-Digest** - Enable Message-Digest Authentication on the OSPF Interface. **Message Digest Key** - Enter key, with a maximum 8 characters. **Message Digest Key ID** - Enter Key ID, with a range of 1-255. **Using Area Authentication** - Enable OSPF area authentication. See *OSPF* on page 2-47 for information about configuring OSPF area authentication.
Interface Parameter	
Retransmit Interval	Defines the interval of time between link state advertisement retransmissions for adjacencies belonging to the interface. Range is 1-65536 seconds, with a default of 5.
Transmit Delay	Defines the estimated time to transmit a link state update packet on the interface. Range is 1-65535 seconds, with a default of 1.
Dead Interval	Defines the interval of time that no hello packets have been seen before neighbors declare the router down. Range is 0-65535 seconds, with a default of 40. **Note:** This value must be the same for all nodes on the network.
Hello Interval	Defines the interval of time between hello packets that the Adit sends on the interface.Range is 0-6553516383 seconds, with a default of 10. **Note:** This value must be the same for all nodes on the network.

Interface Cost	Defines the cost of sending a packet on this interface. Range is 1-65535, with a default of 0.
Interface Priority	Defines the router priority, which determines the designated router for this network. Enter an ID for this key. Range is 1-255, with a default of 1.

CHAPTER 4

Security

In this Chapter

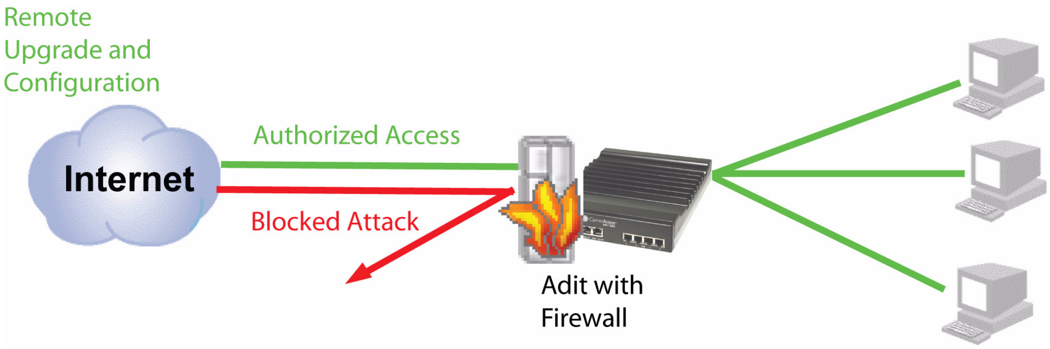
- Overview
- General
- Access Control
- Local Servers
- DMZ Host
- Port Triggering
- Remote Administration
- IP/Hostname Filtering
- Advanced Filtering
- NAT Bypass
- Security Log
- Firewall Implementation

Overview

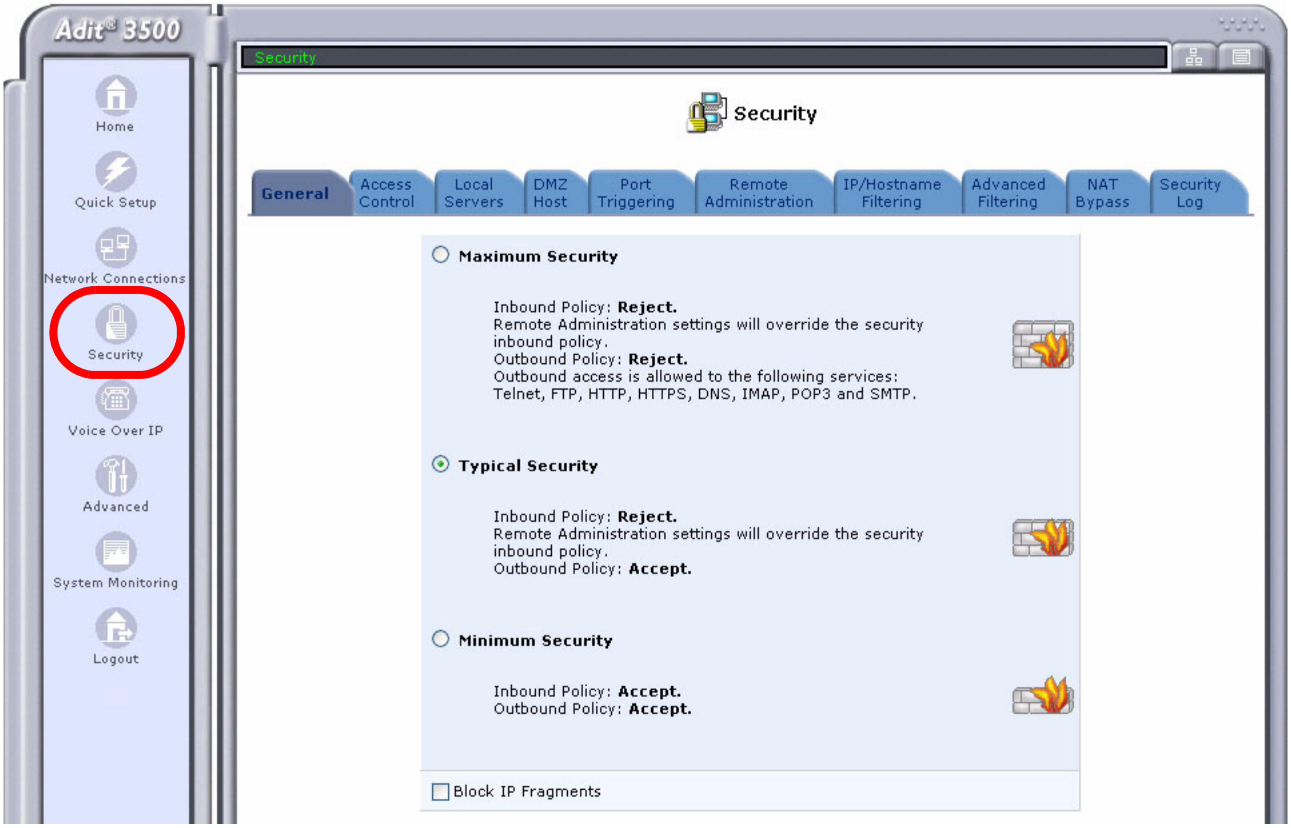
The Adit 3000 and MSR include comprehensive and robust security services:

- Stateful packet inspection firewall
- User authentication protocols
- Password protection mechanisms

The firewall provides both the security and flexibility that users seek and is preconfigured to provide optimum security. It supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. The user can define specific input and output rules, control the order of logically similar sets of rules, and make a distinction between rules that apply to WAN and LAN network devices.



.



Security

○ **Maximum Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services:
Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ **Minimum Security**

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

□ Block IP Fragments

The following sections describe each of the tabs available at the Security window:

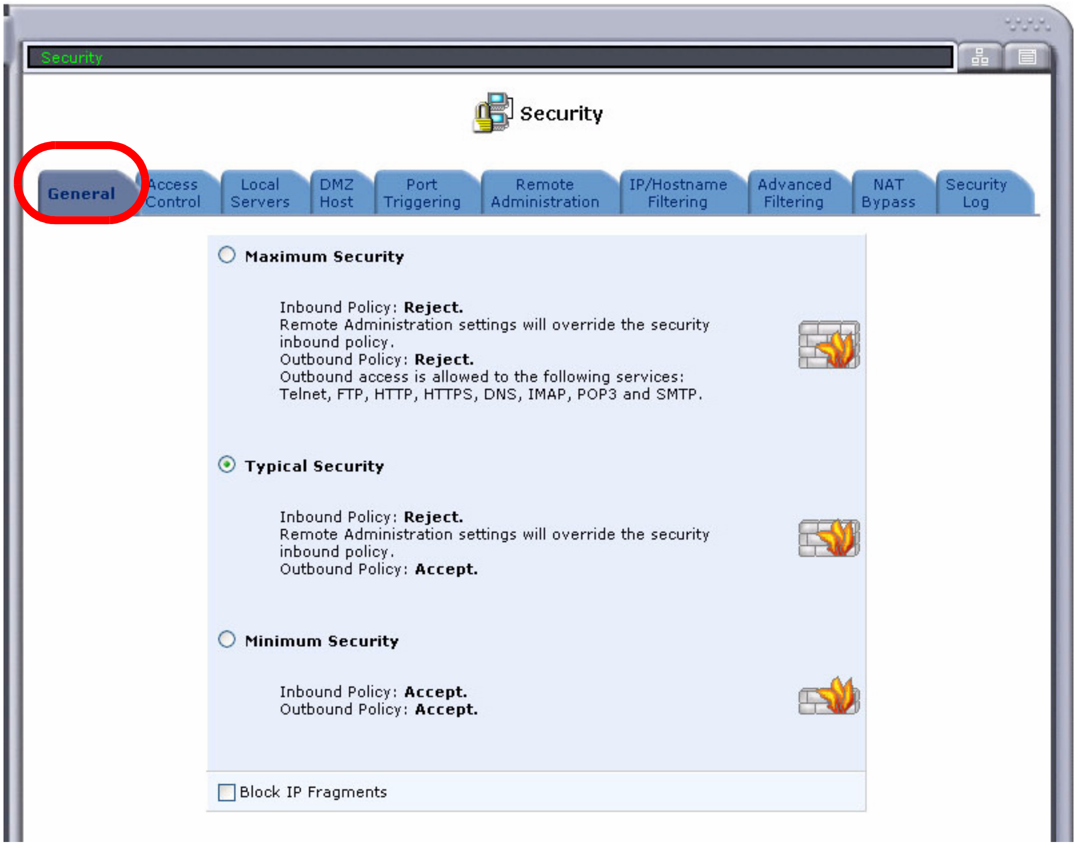
- General
- Access Control
- Local Servers
- DMZ Host
- Port Triggering
- Remote Administration
- IP/Hostname Filtering
- Advanced Filtering
- NAT Bypass
- Security Log

In addition, the following section provides firewall implementation details for users who need more in-depth information:

- Firewall Implementation

General

Use the **General** tab to configure the Adit's basic security settings.



○ **Maximum Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services:
Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

○ **Minimum Security**

Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

□ Block IP Fragments

The firewall regulates the flow of data between the network and the Internet. Both incoming and outgoing data are inspected and then accepted (allowed to pass through the Adit) or rejected (barred from passing through the Adit) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside while allowing users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the network and what types of services available in the network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating from the Internet or from a computer in the network, must be checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, all subsequent data associated with this request (session) will also be allowed to pass, regardless of its direction.

For example, when you point your web browser to a web page on the Internet, a request is sent out to the Internet for this page. When the request reaches the Adit, the firewall identifies the request type and origin (HTTP and a specific PC in your network, in this case). Unless you have configured access control to block requests of this type from this computer, the firewall allows this request to pass out onto the Internet. When the web page is returned from the web server, the firewall associates it with this session and allows it to pass, regardless of whether HTTP access from the Internet to the network is blocked or permitted.

The important thing to note is that it is the origin of the request, not subsequent responses to this request, that determines whether a session can be established or not.

You can choose from among three pre-defined security levels: Minimum, Typical (default setting), and Maximum. The following table defines the behavior of the Adit for each of the three security levels.

NOTE: Using the **Minimum Security** setting may expose the network to significant security risks, and thus should only be used when necessary, for short periods of time.

Security Levels

The following are the security levels available:

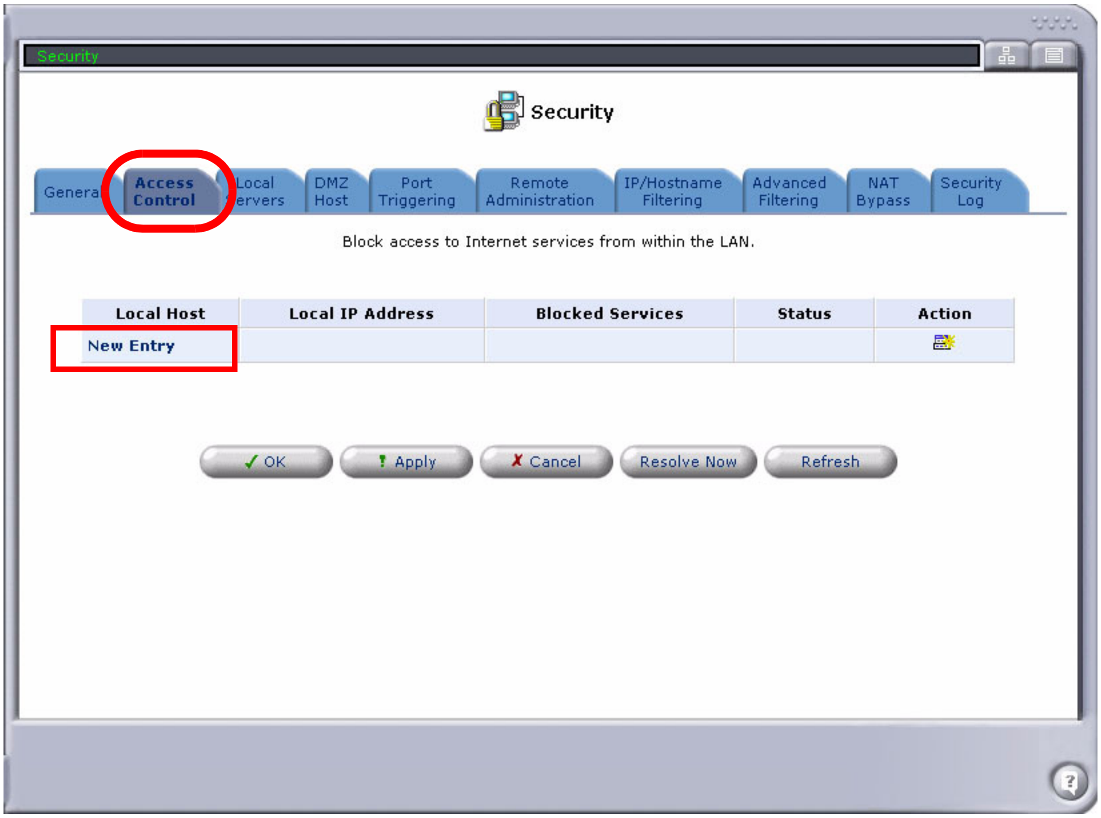
Security Level	Requests Originating in the WAN	Requests Originating in the LAN
Maximum	**Blocked**: No access to network from Internet, except as configured in the Local Servers, DMZ host and Remote Access screens.	**Limited**: Only commonly-used services, such as Web-browsing and e-mail, are permitted. These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, Ping and SNMP.
Typical (Default)	**Blocked**: No access to network from Internet, except as configured in the local Servers, DMZ host and Remote Access screens.	**Unrestricted**: All services are permitted, except as configured in the Access Control screen.
Minimum	**Unrestricted**: Permits full access from Internet to network; all connection attempts permitted.	**Unrestricted**: All services are permitted, except as configured in the Access Control screen.

Field	Definition
Block IP Fragments	Checking this box will protect your network from a common type of hacker attack that could make use of fragmented data packets to sabotage your network. **Note:** VPN over IPSec and some UDP-based services make legitimate use of IP fragments. You will need to allow IP fragments to pass into the home network in order to make use of these selected services.

Access Control

Use the **Access Control** tab to define a rule to block specific network devices within the network from accessing certain services on the Internet. For example, you might prohibit one computer from surfing the Web, another from transferring files using FTP, or the whole network from receiving incoming e-mails.

Access controls work by placing restrictions on the types of requests that may pass from the network out to the Internet and thus may block traffic flowing in both directions.



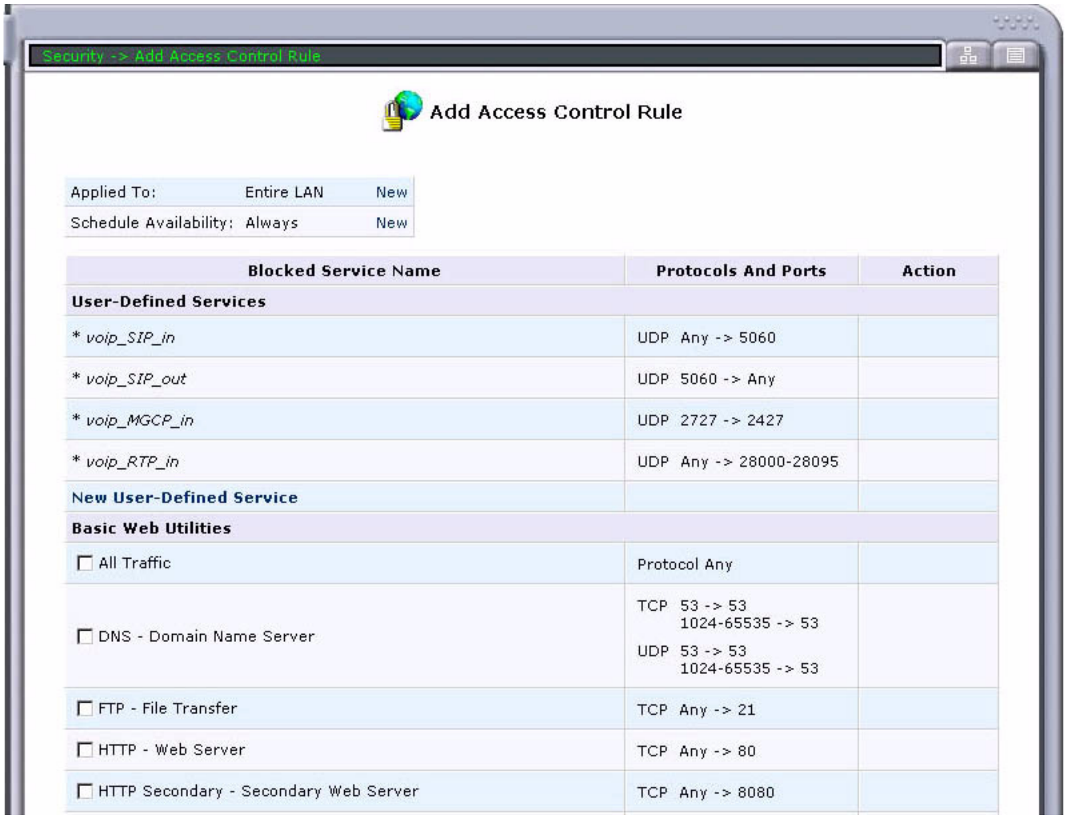
Block access to Internet services from within the LAN.

Local Host	Local IP Address	Blocked Services	Status	Action
New Entry				

Adding an Access Control Rule

To add an access control rule:

1. Select **New Entry** on the **Security/Access Control** window to display the **Add Access Control Rule** window. At this window, you will define what interface to apply the rule to, the time parameters, and the services to be blocked.



Security -> Add Access Control Rule

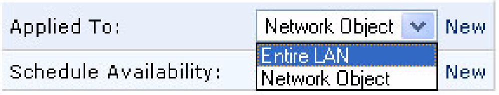
Add Access Control Rule

Applied To:	Entire LAN	New
Schedule Availability:	Always	New

Blocked Service Name	Protocols And Ports	Action
User-Defined Services		
* *voip_SIP_in*	UDP Any -> 5060	
* *voip_SIP_out*	UDP 5060 -> Any	
* *voip_MGCP_in*	UDP 2727 -> 2427	
* *voip_RTP_in*	UDP Any -> 28000-28095	
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	
□ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
□ FTP - File Transfer	TCP Any -> 21	
□ HTTP - Web Server	TCP Any -> 80	
□ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	

⋮

2. Select a Network Object from the **Applied To** pulldown menu (located at the top of the window), or select **New** to define a new Network Object that will be displayed in the pulldown menu. (See *Network Objects on page 2-34* for more information.) **Note:** The pulldown menu is only available when more than one Network Object has been created.



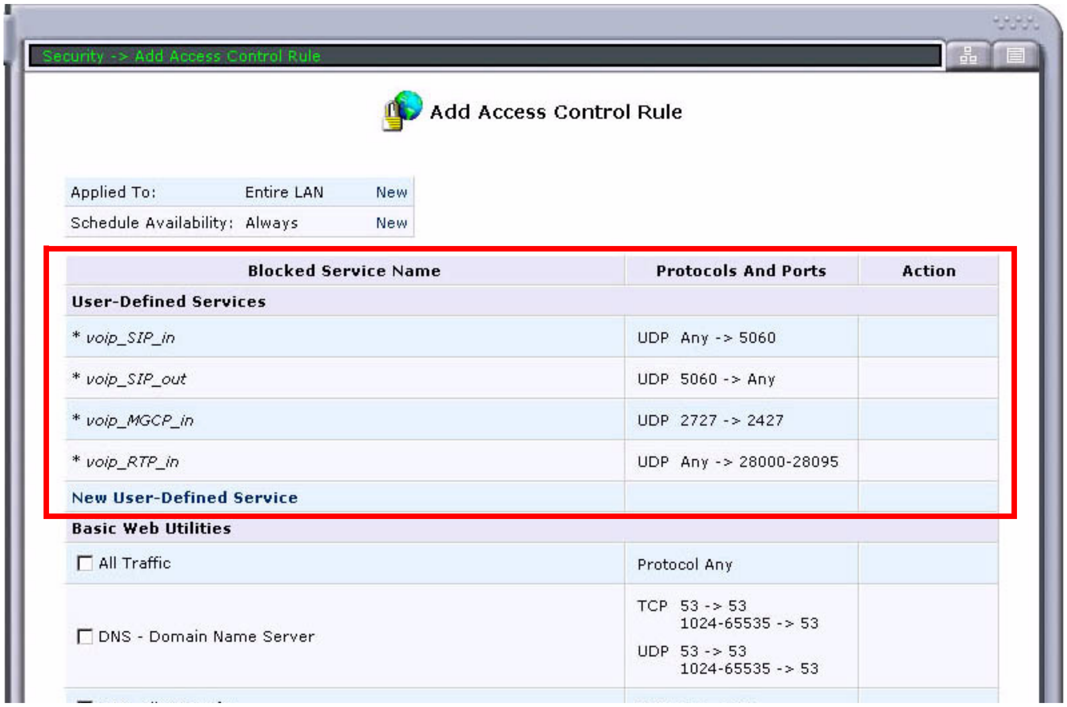
Applied To:	Network Object	New
Schedule Availability:		New

3. **Scheduled Availability -** To set this to a setting other that **Always**, select **New** and specify the schedule on the Schedule Rule Edit window. For information on configuring the schedule, see *Scheduler Rules on page 2-52.*

4. Select the service(s) to block.
   Note: The Service table is used by multiple windows; the standard services and the User-Defined services created on any of these windows will appear here.

NOTE: To block a service that is not included in the list, select **New User-Defined Service**, then define and save the service. See *Creating a User-Defined Rule on page 4-10* for more information.

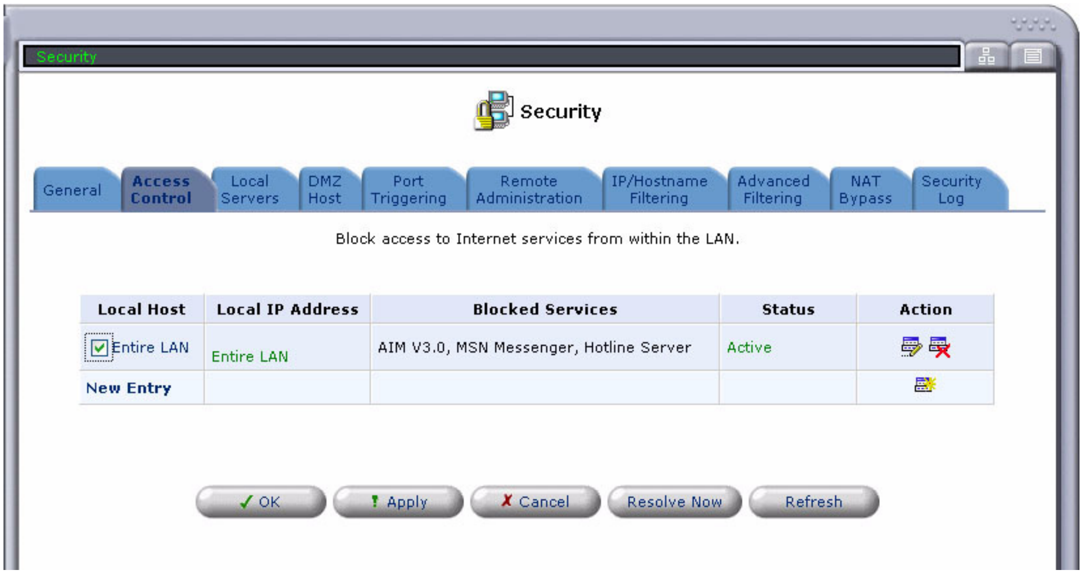
Service table is referenced from multiple windows



Applied To:	Entire LAN	New
Schedule Availability:	Always	New

Blocked Service Name	Protocols And Ports	Action
User-Defined Services		
* *voip_SIP_in*	UDP Any -> 5060	
* *voip_SIP_out*	UDP 5060 -> Any	
* *voip_MGCP_in*	UDP 2727 -> 2427	
* *voip_RTP_in*	UDP Any -> 28000-28095	
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	
□ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	

5. Select **OK** to save the rule. The rule appears in the Access Control table, with a checkbox. The rule can be enabled/disabled, without affecting the rule.

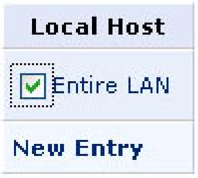


Block access to Internet services from within the LAN.

Local Host	Local IP Address	Blocked Services	Status	Action
☑ Entire LAN	Entire LAN	AIM V3.0, MSN Messenger, Hotline Server	Active	
New Entry				

Modifying an Access Control Rule

- Rules can be enabled/disabled by checking/unchecking the rule listed on the Security window.



Local Host

☑ Entire LAN

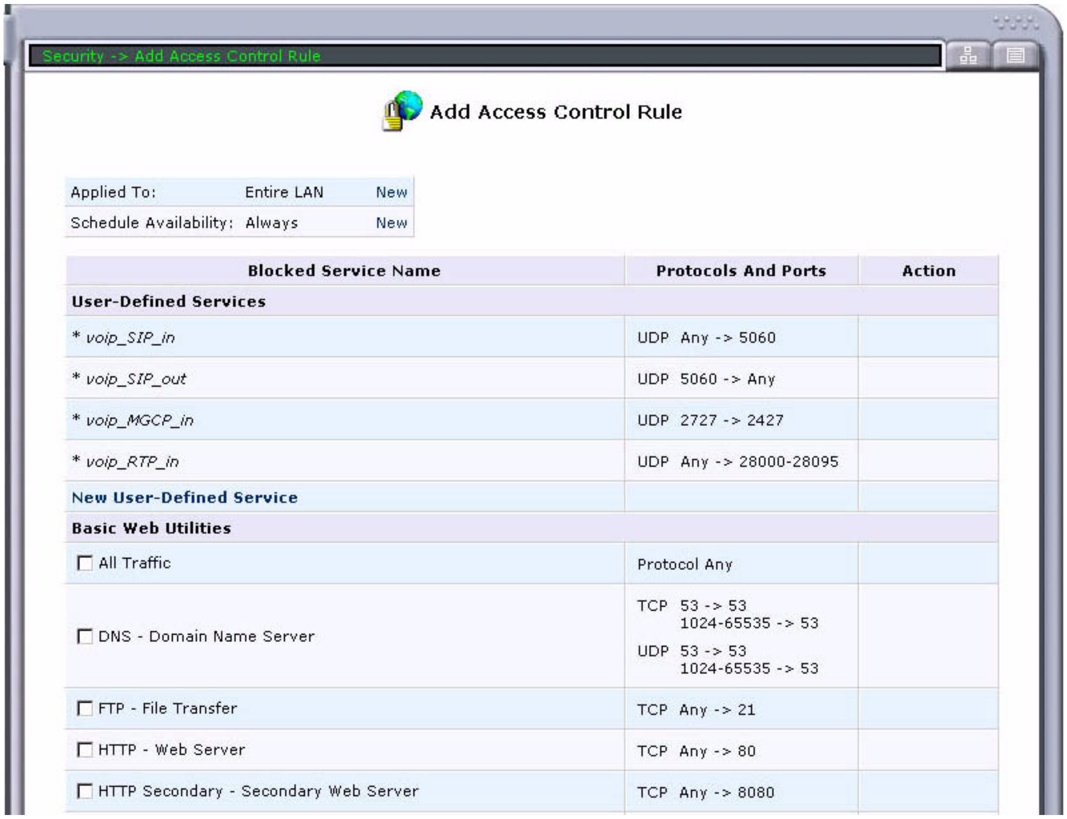
New Entry

- Rules can be modified by selecting the **Edit** button for the rule and modifying the configuration.

- Rules can be deleted by selecting the **Delete** button for the rule.

Creating a User-Defined Rule

1. At the **Add Access Control Rule** window, select the **New User-Defined Service** field.

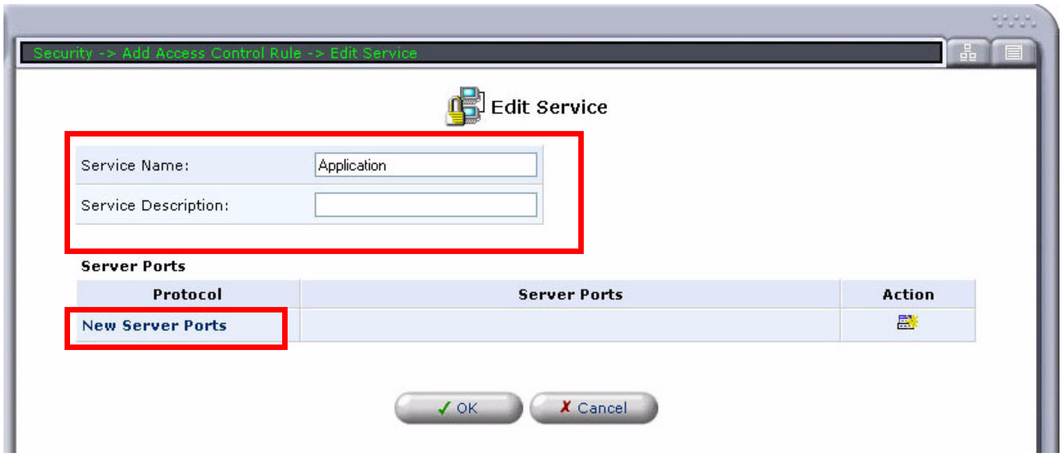


Add Access Control Rule

Applied To:	Entire LAN	New
Schedule Availability:	Always	New

Blocked Service Name	Protocols And Ports	Action
User-Defined Services		
* *voip_SIP_in*	UDP Any -> 5060	
* *voip_SIP_out*	UDP 5060 -> Any	
* *voip_MGCP_in*	UDP 2727 -> 2427	
* *voip_RTP_in*	UDP Any -> 28000-28095	
New User-Defined Service		
Basic Web Utilities		
☐ All Traffic	Protocol Any	
☐ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
☐ FTP - File Transfer	TCP Any -> 21	
☐ HTTP - Web Server	TCP Any -> 80	
☐ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	

2. Name the service and give a description, if needed.



Edit Service

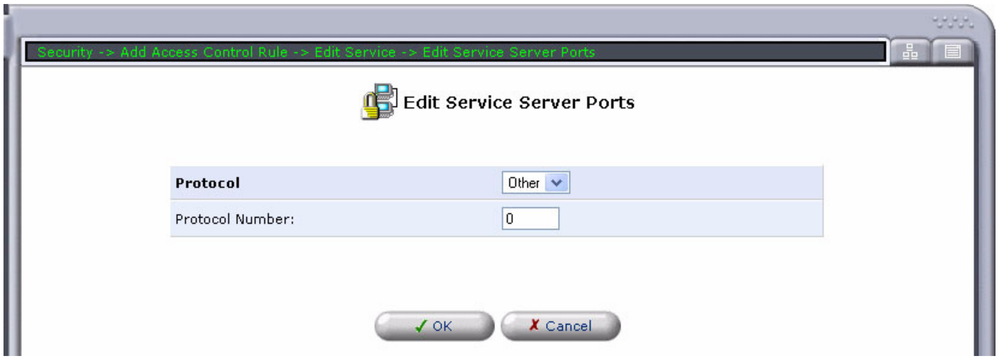
Service Name:	Application
Service Description:	

Server Ports

Protocol	Server Ports	Action
New Server Ports		

3. Select a **Server Port** from the list, or select **New Server Ports** to create one.

4. Configure the Service port protocol:



Security -> Add Access Control Rule -> Edit Service -> Edit Service Server Ports

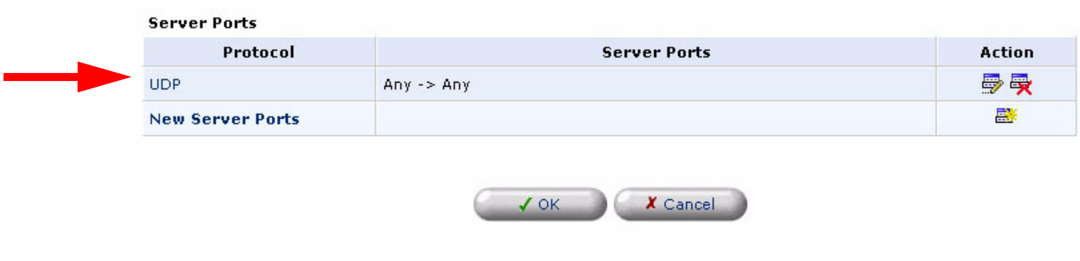
Edit Service Server Ports

Protocol	Other
Protocol Number:	0

Field	Definition
Protocol	**TCP** - Transmission Control Protocol. TCP is a transport layer, connection-oriented, end-to-end protocol. It provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user. Source Ports and Destination Ports: **Any** - Applies to any port. **Single** - Enter specific port (range 0 - 65535) **Range** - Enter Range of ports (range 0 - 65535)
	UDP - User Datagram Protocol. UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery. **Note:** UDP is part of the TCP/IP protocol suite. Source Ports and Destination Ports: **Any** - Applies to any port. **Single** - Enter specific port (range 0 - 65535) **Range** - Enter Range of ports (range 0 - 65535)
	ICMP - Internet Control Message Protocol. ICMP allows router to send error and control messages about packet processing on IP networks. **Note:** ICMP is part of the TCP/IP protocol suite. ICMP message to send: **Echo Reply** **Network Unreachable** **Host Unreachable** **Protocol Unreachable** **Port Unreachable** **Destination Network Unknown** **Destination Host Unknown** **Redirect for Network** **Redirect for Host** **Echo Request** **Other:** **ICMP Type -** Range is 0 - 255 **ICMP Code** - Range is 0 - 255
	GRE - Generic Routing Encapsulation. GRE provides for the encapsulation of one data packet inside another data packet.
	ESP - Encapsulating Security Payload. The portion of the IPSec virtual private networking protocol which is used predominantly to provide data privacy.

Field	Definition (Continued)
	AH - Authentication Header Protocol. A protocol used in IPSec that authenticates a packet IP header and payload (content). If a packet is modified during transmission, the recipient is notified.
	Other - Covers protocols not listed above. This option requires a **Protocol Number** to be entered. Range is 0- 65535.

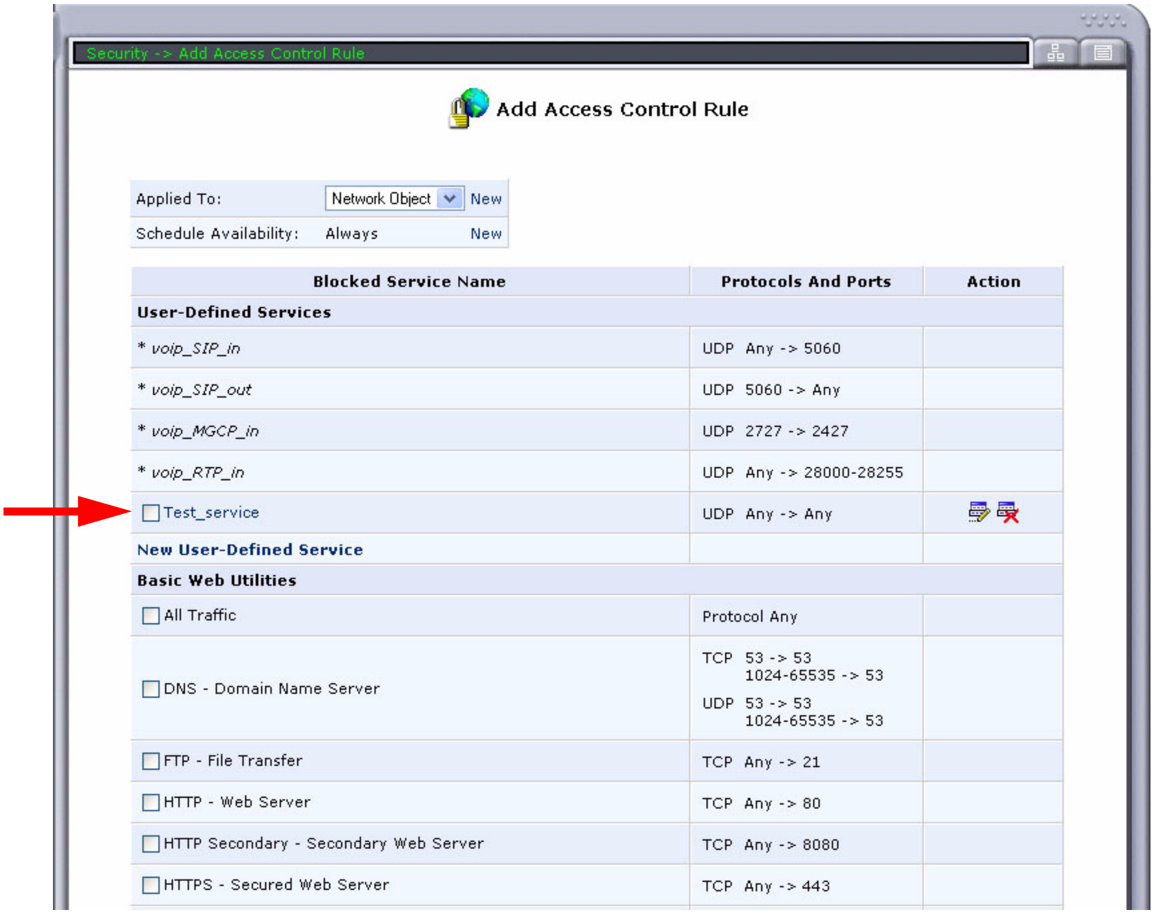
5. Select **OK** to save. The newly created service port is listed in the table.



Server Ports

Protocol	Server Ports	Action
UDP	Any -> Any	
New Server Ports		

6. Select **OK** to save the User-Defined Service. The new service is listed (with a checkbox) in the table.



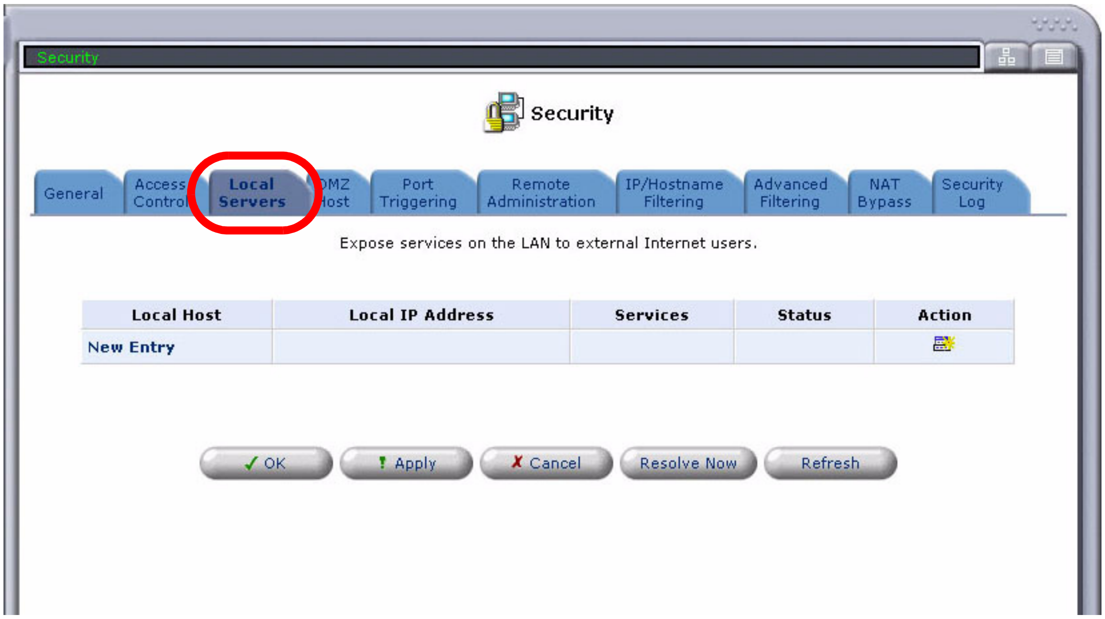
Add Access Control Rule

Applied To:	Network Object	New
Schedule Availability:	Always	New

Blocked Service Name	Protocols And Ports	Action
User-Defined Services		
* *voip_SIP_in*	UDP Any -> 5060	
* *voip_SIP_out*	UDP 5060 -> Any	
* *voip_MGCP_in*	UDP 2727 -> 2427	
* *voip_RTP_in*	UDP Any -> 28000-28255	
□ Test_service	UDP Any -> Any	
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	
□ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
□ FTP - File Transfer	TCP Any -> 21	
□ HTTP - Web Server	TCP Any -> 80	
□ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	
□ HTTPS - Secured Web Server	TCP Any -> 443	

Local Servers

By default, the Adit blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may need to expose your network to the Internet in certain limited and controlled ways to enable some applications to work from the LAN and to establish servers in the network. The Local Servers feature supports both of these functions. If you are familiar with networking terminology and concepts, you may have encountered this topic referred to as Port Forwarding.



Expose services on the LAN to external Internet users.

Local Host	Local IP Address	Services	Status	Action
New Entry				

The **Local Servers** tab on the Security window provides access to a list of the most commonly used applications that require handling by the Adit. All you have to do is identify which of them you want to use and the local IP address of the computer that will be using the service. For example, if you want to use the Net2Phone voice application on one of your PCs, simply select Net2Phone from the list and enter the local IP address of that computer in the **Local Host** field. All Net2Phone-related data arriving at the Adit from the Internet will be forwarded to the specified computer.

Similarly, if you want to grant Internet users access to servers inside your network, you must identify each service that you want to provide and the PC that will provide it. For example, if you want to host a Web server inside the network, select **HTTP - Web Server** from the list and enter the local IP address of the computer that will host the Web server in the **Local Host** field. Then, when a an Internet user points the browser to the external IP address of the Adit, the Gateway will forward the incoming HTTP request to the computer that is hosting the Web server.

Local Servers is a NAPT function. It only applies to packets whose destination address is the Adit's own WAN IP address. When a local server match is applied, packets are redirected from the Adit WAN IP address to the local server's IP address. Note that the Local Servers are active if either the firewall is enabled on the WAN interface or the WAN interface routing type is set for NAPT.

Additionally, Local Servers enable you to redirect traffic to a port different than the specified port. For example, if you have a web server running on your PC on port 8080, and you want to grant access to this server to anyone who accesses the Adit via HTTP, you can do the following:

- Define a **Local Host** for the HTTP service, with the PC's IP or hostname.
- Specify 8080 in the **Forwarded Port** field.

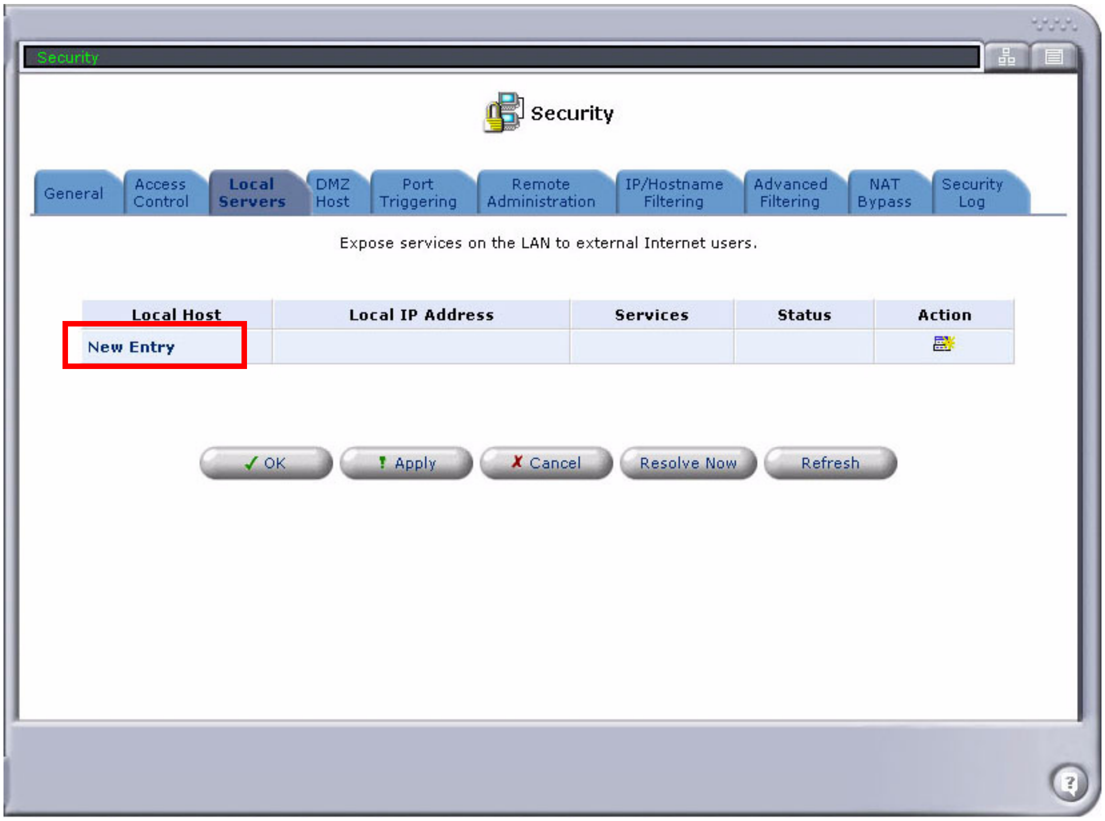
All incoming HTTP traffic will be forwarded to the PC running the web server on port 8080.

NOTE: If an Internet application or a service that you wish to provide is not in the list, you can easily add it.

Adding a Local Server

To add a a new server to the list of active local servers:

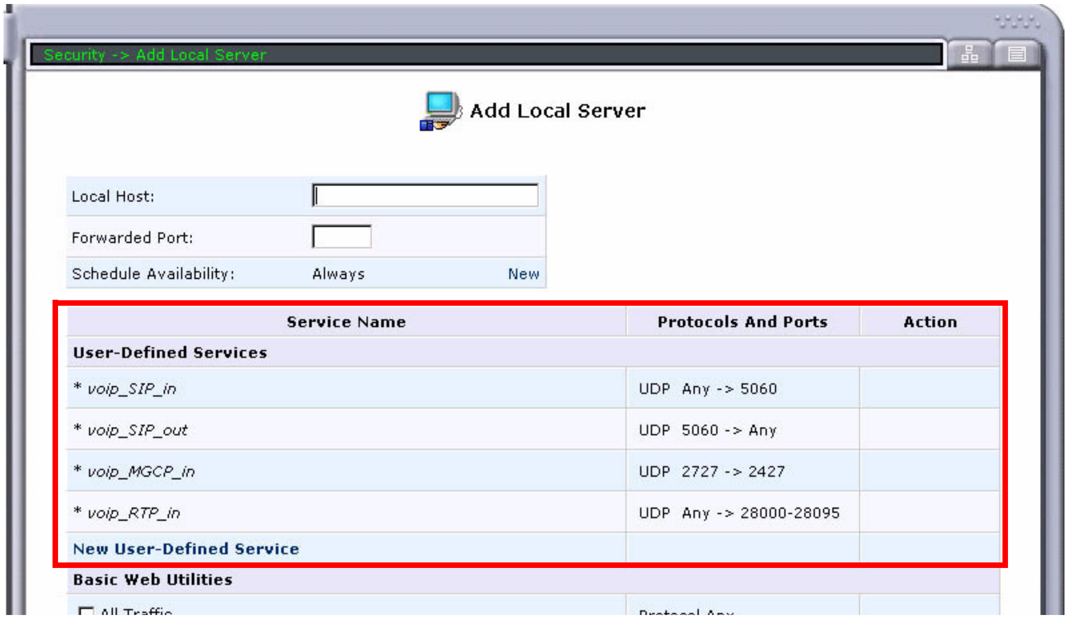
1. Select **New Entry** on the **Security/Local Server** window.



Expose services on the LAN to external Internet users.

Local Host	Local IP Address	Services	Status	Action
New Entry				

2. Enter the local IP address of the computer that will provide the service (server) in the **Local Host field**. **Note:** Only one LAN computer an be assigned to provide a specific service or application.
3. Enter a forwarding port in the **Forwarded Port** field. Range is 0 - 65535.
4. **Scheduled Availability** - To set this to a setting other that **Always**, select **New** and specify the schedule on the Schedule Rule Edit window. For information confguring the schedule, see *Scheduler Rules on page 2-52.*
5. Select the service you would like to provide.
Note: The Service table is used by multiple windows; the standard services and the User-Defined services created on any of these windows appear here.

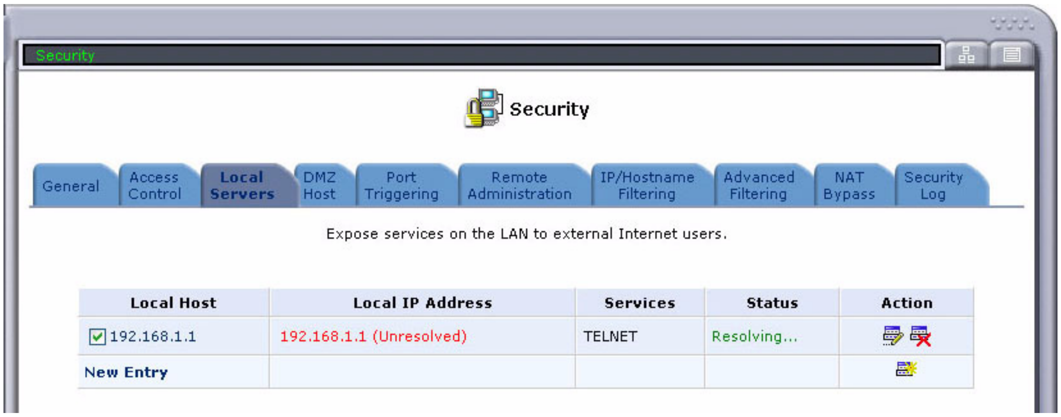


Service table is referenced from multiple windows

Local Host:		
Forwarded Port:		
Schedule Availability:	Always	New

Service Name	Protocols And Ports	Action
User-Defined Services		
* *voip_SIP_in*	UDP Any -> 5060	
* *voip_SIP_out*	UDP 5060 -> Any	
* *voip_MGCP_in*	UDP 2727 -> 2427	
* *voip_RTP_in*	UDP Any -> 28000-28095	
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	

6. Select **OK** to save. The new Local Server is listed in the table.

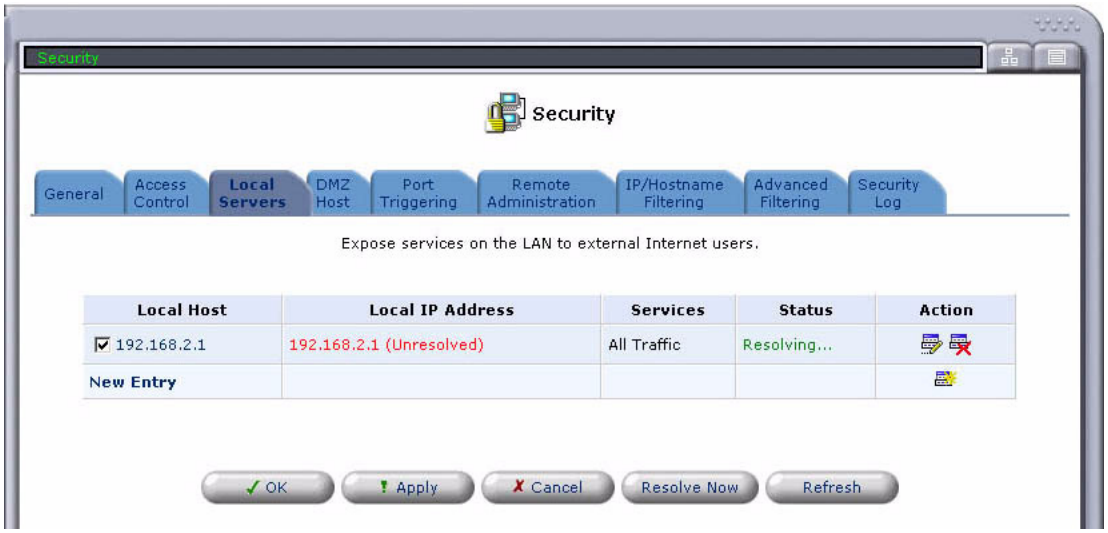


Expose services on the LAN to external Internet users.

Local Host	Local IP Address	Services	Status	Action
☑ 192.168.1.1	192.168.1.1 (Unresolved)	TELNET	Resolving...	
New Entry				

NOTE: To block a service that is not included in the list, select **New User-Defined Service**, then define and save the service. See *Creating a User-Defined Rule on page 4-10*.

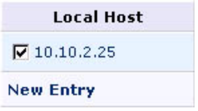
Modifying a Local Server



Expose services on the LAN to external Internet users.

Local Host	Local IP Address	Services	Status	Action
☑ 192.168.2.1	192.168.2.1 (Unresolved)	All Traffic	Resolving...	
New Entry				

- A Local Server can be enabled/disabled by simply checking/unchecking the server listed on the Security window.



Local Host
☑ 10.10.2.25
New Entry

- A Local Server can be modified by selecting the **Edit** button for the server and modifying the configuration.

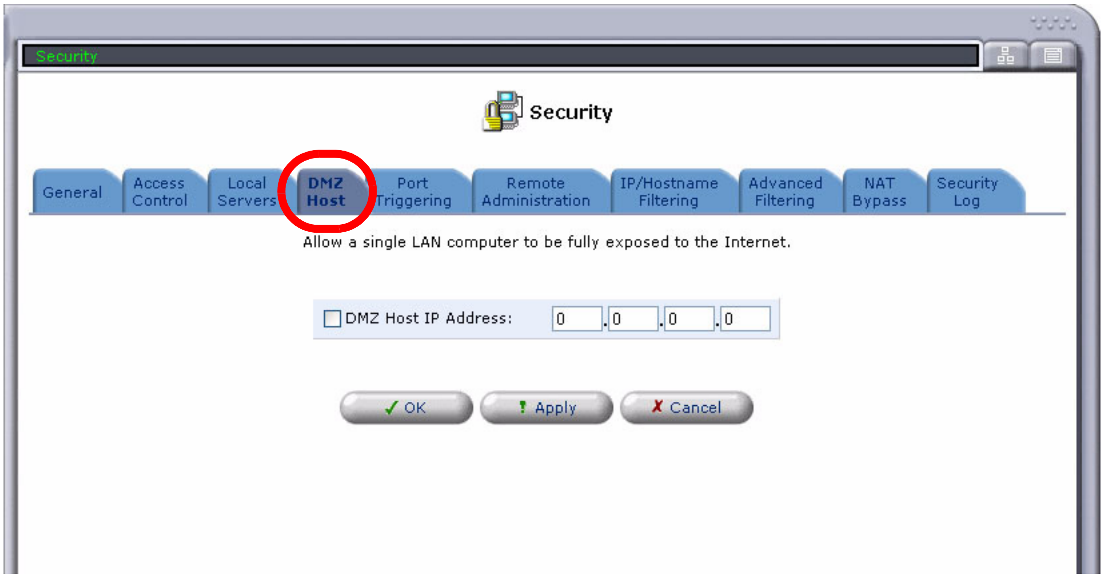
- A Local Server can be deleted by selecting the **Delete** button for the server.

DMZ Host

The DMZ (Demilitarized Zone) Host feature allows one local computer to be exposed to the Internet. Designate a DMZ host when:

- Using a special-purpose Internet service, such as a video-conferencing program, that is not present in the Local Servers list and where no port range information is available.
- You are not concerned with security and choose to expose one computer to all services without restriction.

The DMZ host is an NAPT function. It only applies to packets whose destination address is the Adit's own WAN IP address. It only is utilized when there are no matching Local Servers or Remote Administration matches. When the DMZ Host configuration is applied, packets are redirected from the Adit WAN IP address to the DMZ host's IP address. **Note:** The DMZ Host is only active if the firewall is enabled on the WAN interface, regardless of whether the WAN interface routing type is set for NAPT or Routing.



Allow a single LAN computer to be fully exposed to the Internet.

□ DMZ Host IP Address: 0 . 0 . 0 . 0

WARNING! A DMZ HOST IS NOT PROTECTED BY THE FIREWALL AND MAY BE VULNERABLE TO ATTACK. IT MAY ALSO PUT OTHER COMPUTERS IN THE NETWORK AT RISK. WHEN DESIGNATING A DMZ HOST, YOU MUST CONSIDER THE SECURITY IMPLICATIONS AND PROTECT IT IF NECESSARY.

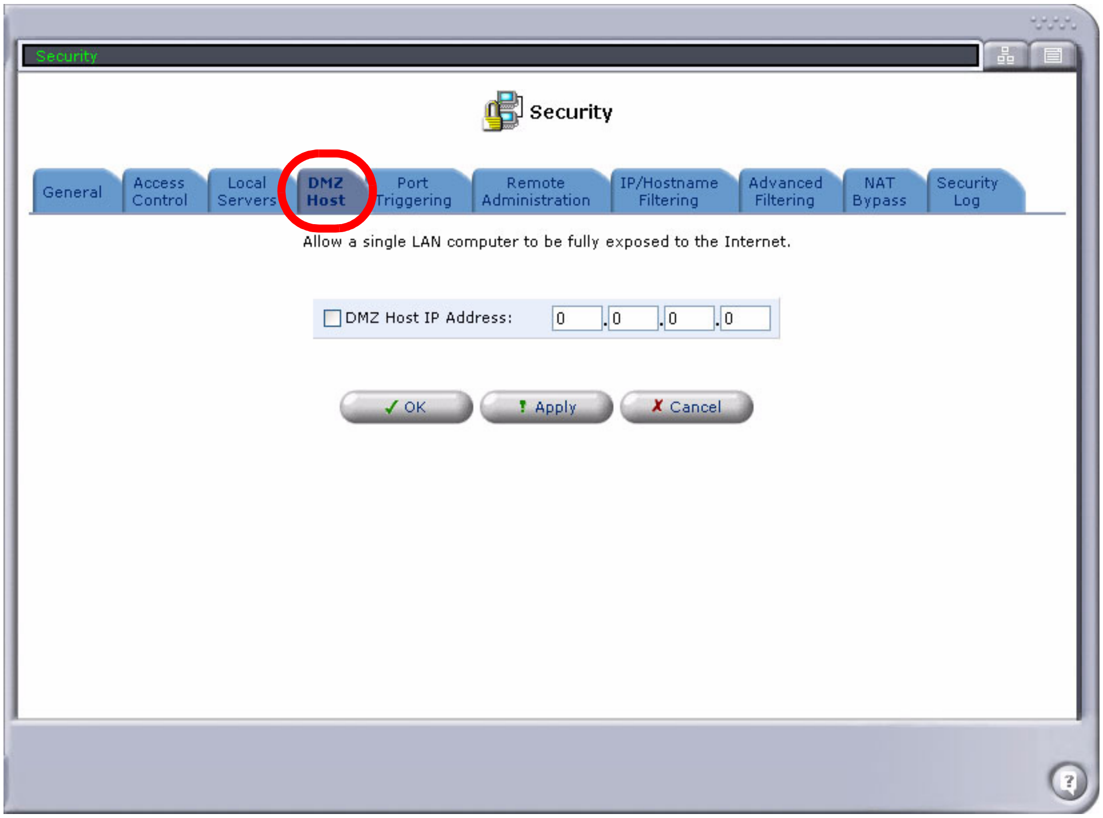
An incoming request for access to a service at the Adit WAN IP address, such as a Web-server, is fielded by the Adit and forwarded to either:

- a matching configured Local Server, or
- a permitted Remote Management session, or
- the DMZ host (if one is designated)

Designating a Local Computer as a DMZ Host

To designate a local computer as a DMZ host, enter the IP address of the computer at the **Security/DMZ Host** window. You can enable/disable the DMZ host at any time by checking/unchecking the checkbox next to the host.

NOTE: Only one LAN computer can be a DMZ host at any time.

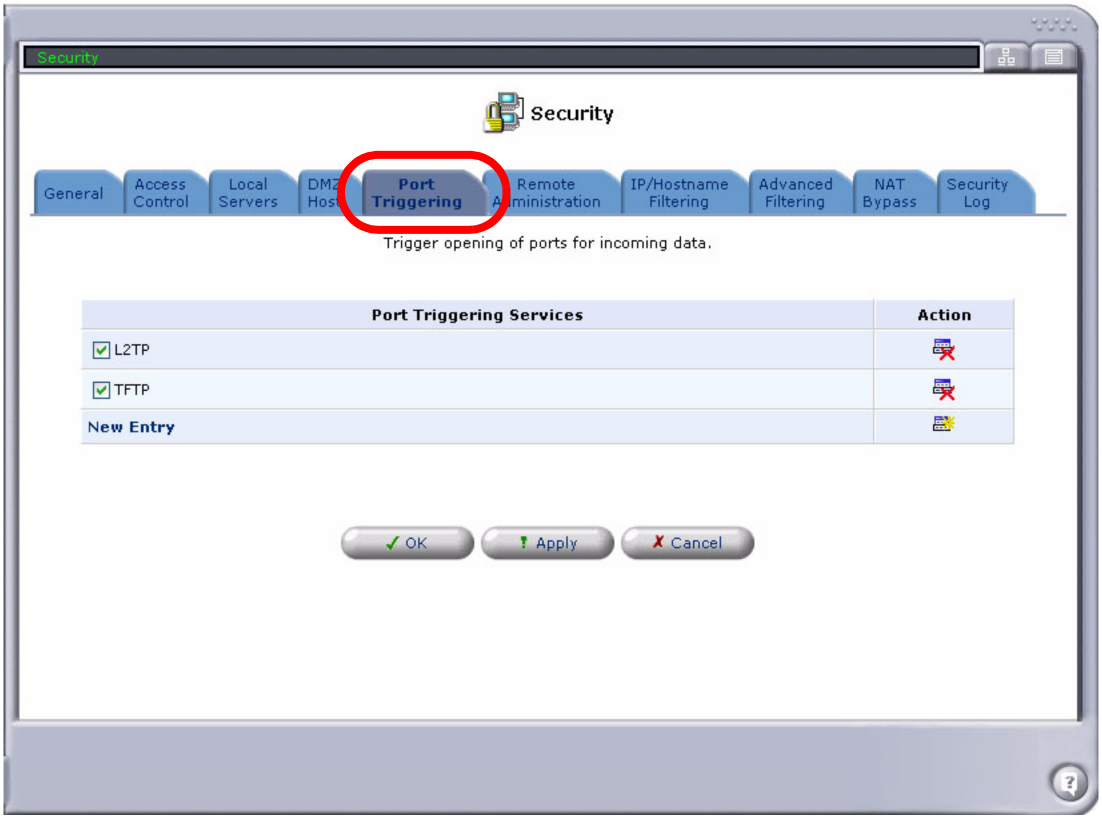


Allow a single LAN computer to be fully exposed to the Internet.

□ DMZ Host IP Address: 0 . 0 . 0 . 0

Port Triggering

Port triggering can be used for dynamic port forwarding. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic.



Trigger opening of ports for incoming data.

Port Triggering Services	Action
☑ L2TP	
☑ TFTP	
New Entry	

For example, you might access a gaming server on port 2222 using the TCP protocol. The gaming server responds by connecting you using TCP on port 3333 to start the gaming session. In such a case, you must use port forwarding since this scenario conflicts with the following default firewall settings:

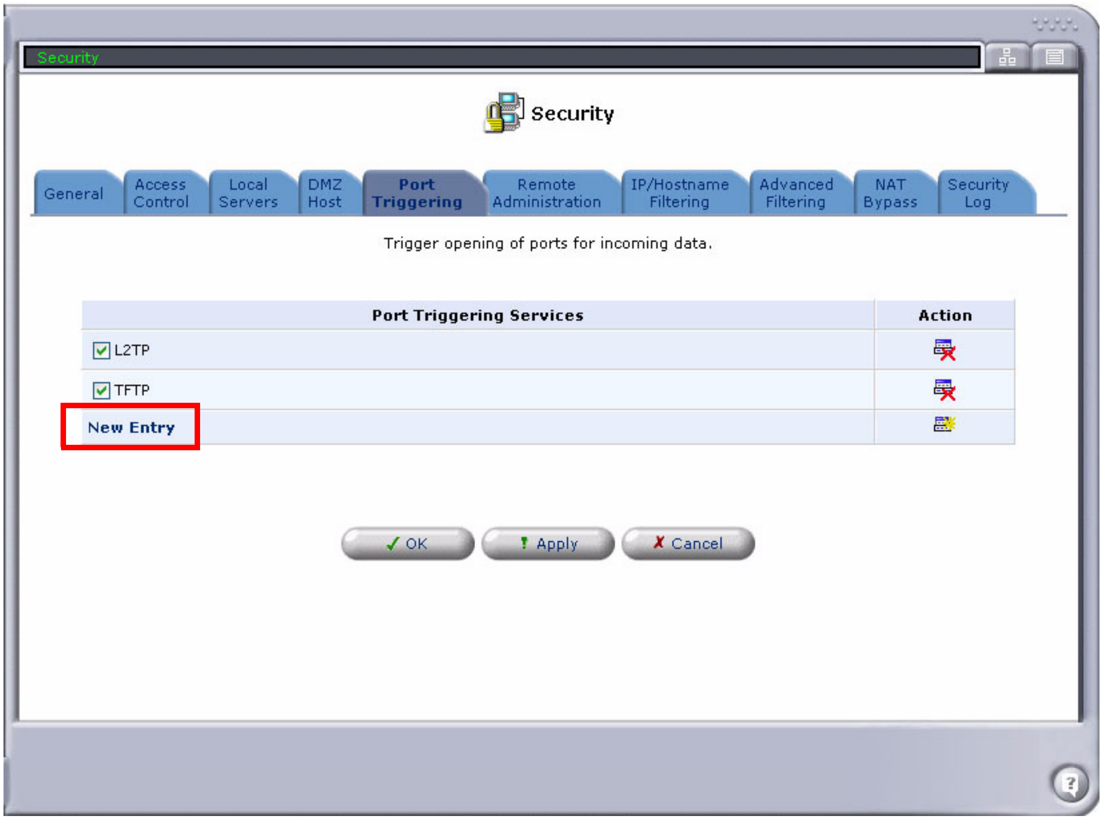
- The firewall blocks inbound traffic by default.
- The server replies to the Adit’s IP, and the connection is not NATed back to your host.

In order to solve this, you need to define a Port Triggering entry that allows inbound TCP traffic on port 3333 only after a LAN host generates TCP traffic to port 2222. This results in accepting the inbound traffic from the gaming server and sending it back to the LAN Host that originated the outgoing traffic on port 2222.

Setting up Port Triggering

To set up port triggering:

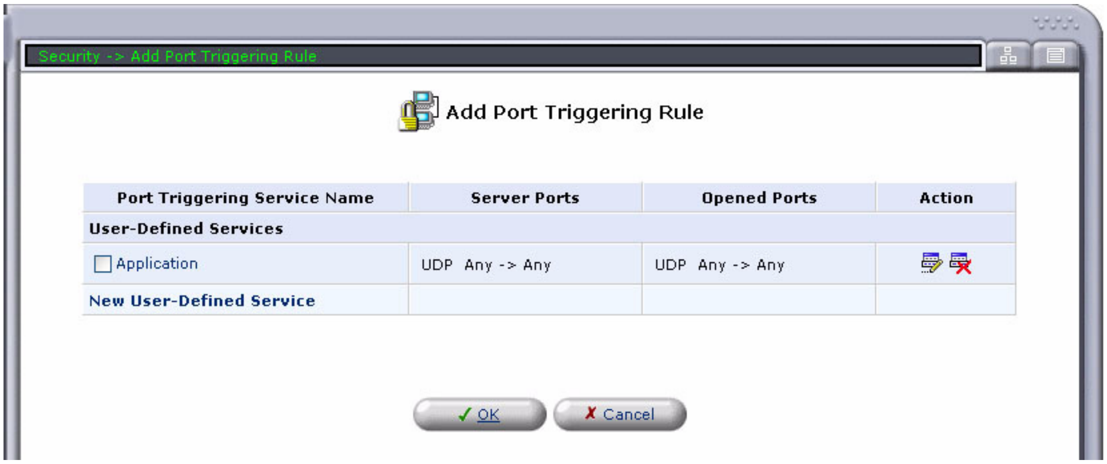
1. Select **New Entry** on the **Security/Port Triggering** window.



Trigger opening of ports for incoming data.

Port Triggering Services	Action
☑ L2TP	
☑ TFTP	
New Entry	

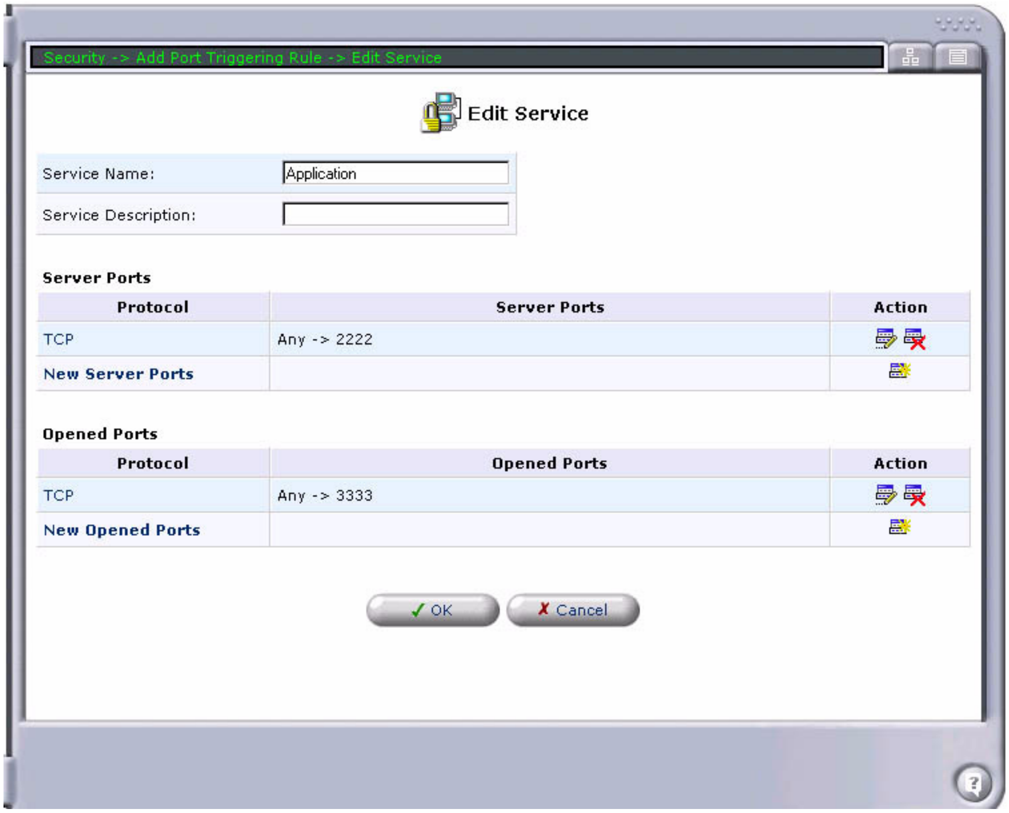
2. Select a previously defined service under **User-Defined Services**, or select **New User-Defined Service**.



Port Triggering Service Name	Server Ports	Opened Ports	Action
User-Defined Services			
□ Application	UDP Any -> Any	UDP Any -> Any	
New User-Defined Service			

3. If creating a **New User-Defined Service**:

    a. Enter a **Service Name** and **Service Description**.



Security -> Add Port Triggering Rule -> Edit Service

Edit Service

Service Name:	Application
Service Description:	

Server Ports

Protocol	Server Ports	Action
TCP	Any -> 2222	
New Server Ports		

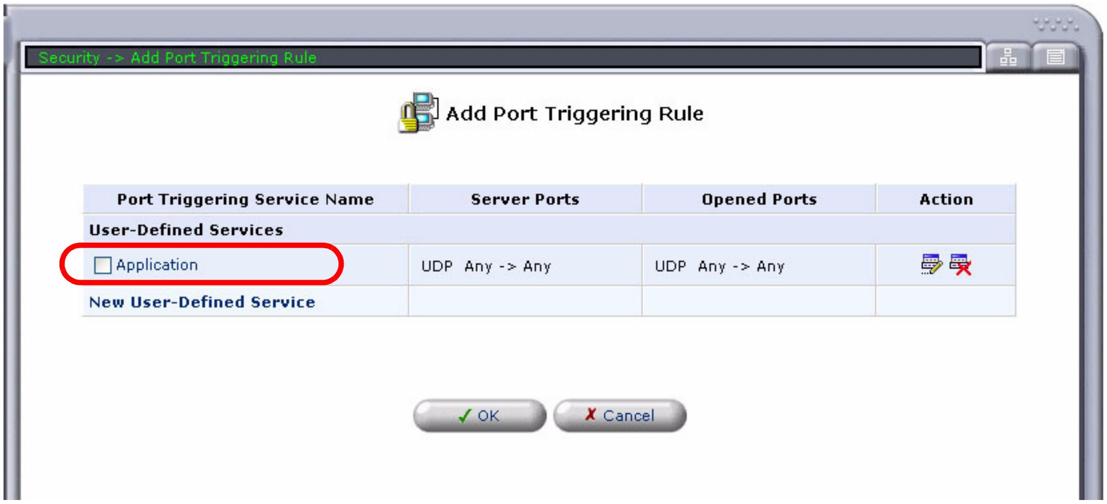
Opened Ports

Protocol	Opened Ports	Action
TCP	Any -> 3333	
New Opened Ports		

    b. Under **Server Ports**, select a configured port from the list, or create a new port by selecting **New Server Ports** (see *Configure the Service port protocol: on page 4-11*).

    c. Under **Opened Ports**, select a configured port from the list, or create a new port by selecting **New Opened Ports** (see *Configure the Service port protocol: on page 4-11*).

d. Select **OK**. The new triggering service is listed in the table.

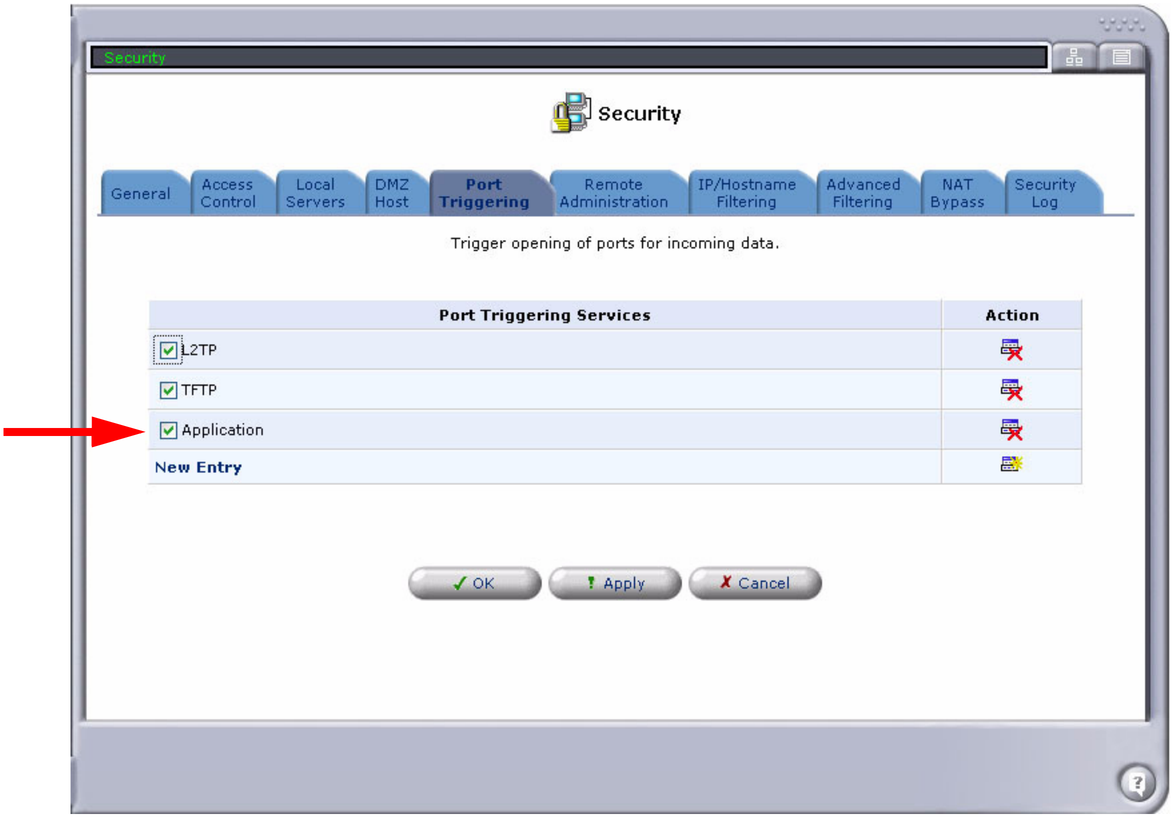


Security -> Add Port Triggering Rule

Add Port Triggering Rule

Port Triggering Service Name	Server Ports	Opened Ports	Action
User-Defined Services			
□ Application	UDP Any -> Any	UDP Any -> Any	
New User-Defined Service			

e. Select the checkbox next to the new service, and select **OK**. The new triggering service is enabled and available for selection. You can enable/disable the service at any time by selecting/un-selecting the checkbox.



Security

Security

Trigger opening of ports for incoming data.

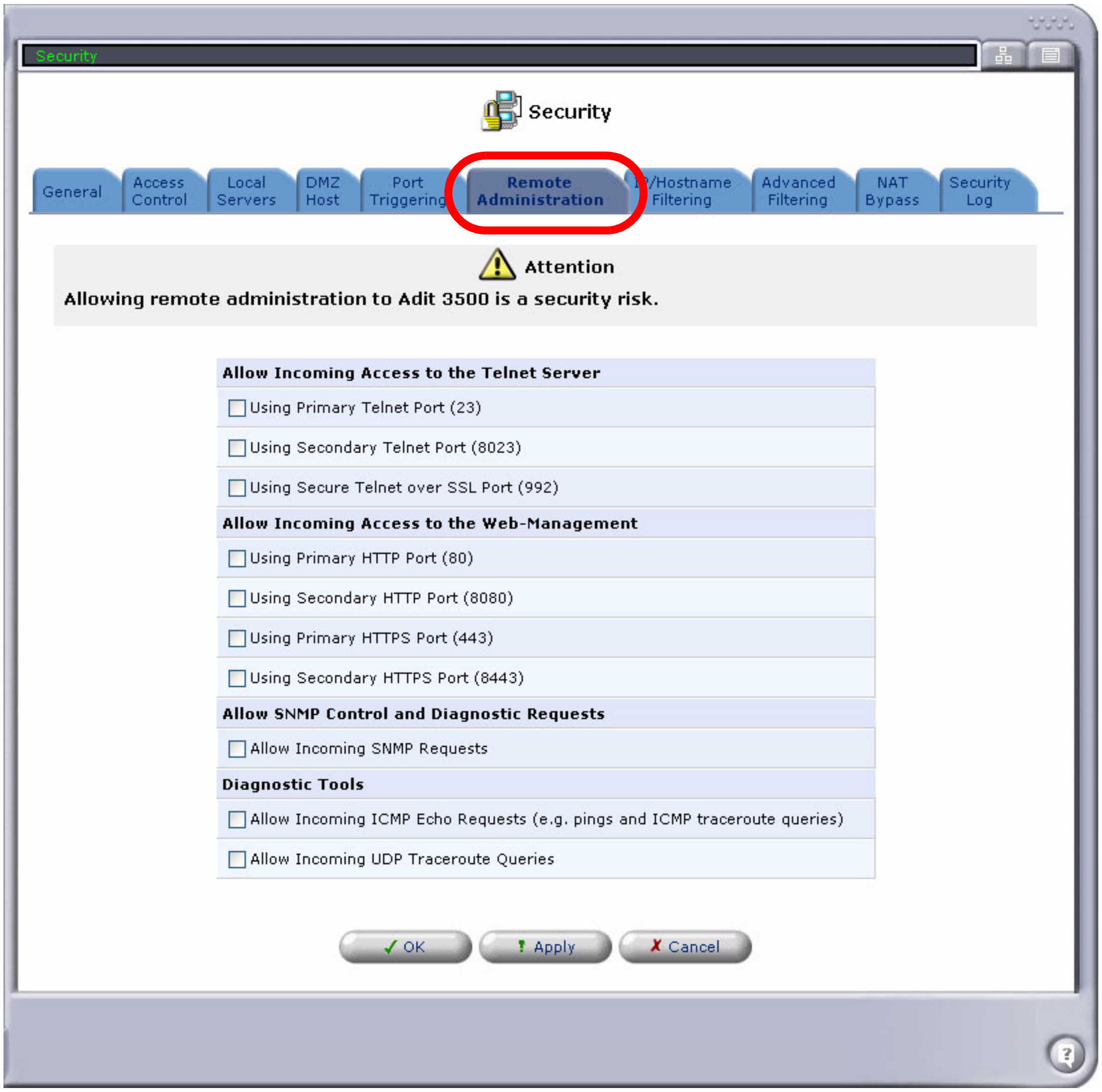
Port Triggering Services	Action
☑ L2TP	
☑ TFTP	
☑ Application	
New Entry	

4. Select **OK**.

Remote Administration

It is possible to access and control the Adit not only from within the network, but also from the Internet. This allows you to view or change settings while traveling. It also enables your ISP to change settings or help you troubleshoot functionality or communication issues from a remote location.

Remote access is blocked by default to ensure the security of your network. However, you can use the **Security/Remote Administration** window to selectively enable a variety of remote administration services as necessary.



Attention
Allowing remote administration to Adit 3500 is a security risk.

Allow Incoming Access to the Telnet Server

- □ Using Primary Telnet Port (23)
- □ Using Secondary Telnet Port (8023)
- □ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the Web-Management

- □ Using Primary HTTP Port (80)
- □ Using Secondary HTTP Port (8080)
- □ Using Primary HTTPS Port (443)
- □ Using Secondary HTTPS Port (8443)

Allow SNMP Control and Diagnostic Requests

- □ Allow Incoming SNMP Requests

Diagnostic Tools

- □ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
- □ Allow Incoming UDP Traceroute Queries

WARNING! ENABLING REMOTE ADMINISTRATION (ACCESS) TO THE ADIT IS A SECURITY RISK AND IS NOT RECOMMENDED.

Configuring Remote Administration

To configure remote access to Adit administration services:

1. Select **Security/Remote Administration**.
2. Select the services that you would like to make available to computers on the Internet. By default, all fields are unselected (disabling all remote services):

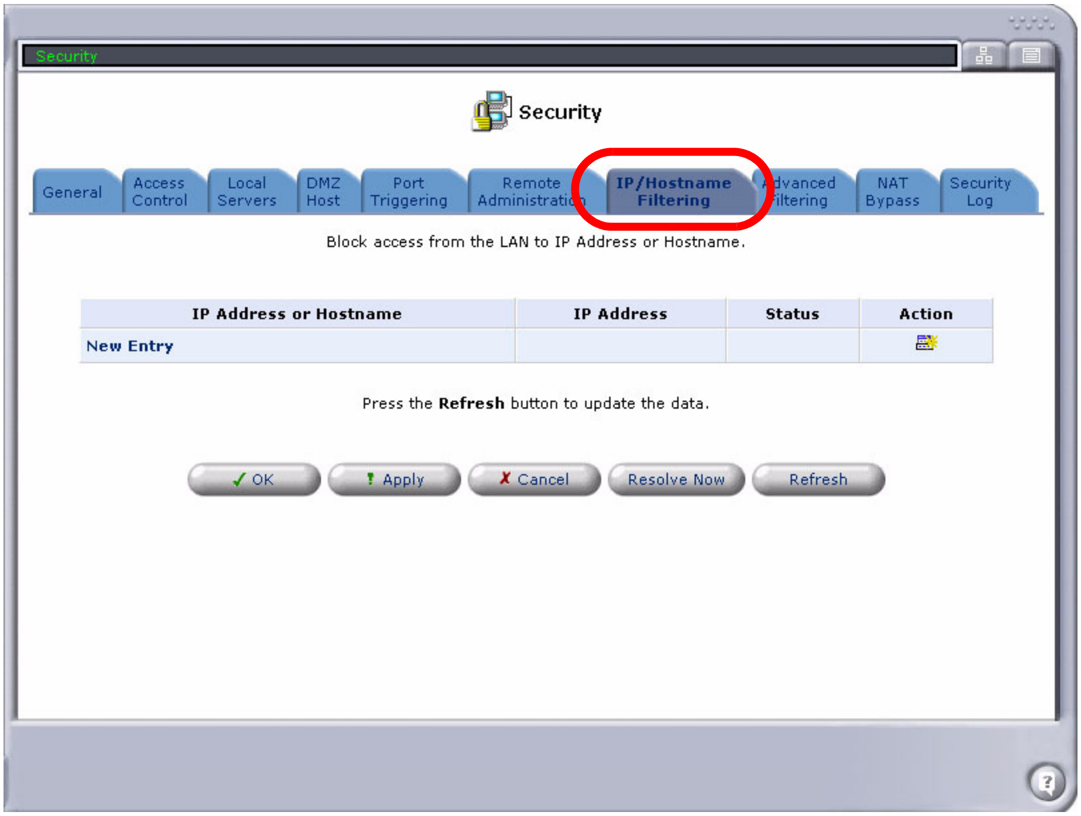
Field	Definition
Allow Incoming Access to the Telnet Server Grants command-line access to the Adit. While this service is password-protected, it is not considered a secure protocol.	
	Using Primary Telnet Port (23)
	Using Secondary Telnet Port (8023) **Note:** If a local server is configured to use port 23, select port 8023 to avoid conflicts.
	Using Secure Telnet over SSL Port (992)
Allow Incoming Access to the Web-Management	
	Using Primary HTTP Port (80)
	Using Secondary HTTP Port (8080)
	Using Primary HTTPS Port (443)
	Using Secondary HTTPS Port (8443)
Allow SNMP Control and Diagnostic Requests	
	Allow Incoming SNMP Requests
Diagnostic Tools Includes Ping and Traceroute (over UDP). These services may be used for troubleshooting and remote system management by the service provider.	
	Allow Incoming ICMP Echo Requests Allows Pings and ICMP traceroute queries.
	Allow Incoming UDP Traceroute Queries Allows UDP traceroute queries.

3. Select **OK**.

IP/Hostname Filtering

You can configure the Adit to block specific IP addresses or hostnames so that they can not be accessed from computers in the network. Moreover, restrictions can be applied to a comprehensive automatically updated list of sites to which access is not recommended.

The **IP/Hostname Filtering** window displays a list of all restricted IP addresses or hostnames.



Block access from the LAN to IP Address or Hostname.

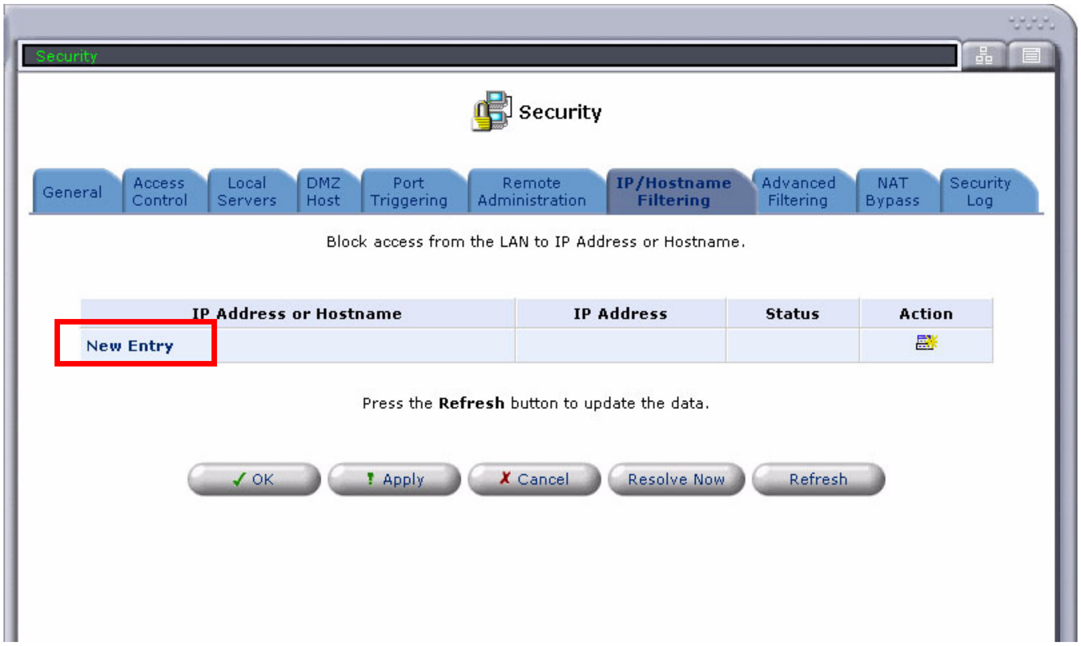
IP Address or Hostname	IP Address	Status	Action
New Entry			

Press the **Refresh** button to update the data.

Adding an Address/Hostname to the Restricted List

To add a restricted IP address or hostname:

1. Select **New Entry** on the **Security/ IP/Hostname Filtering** window.

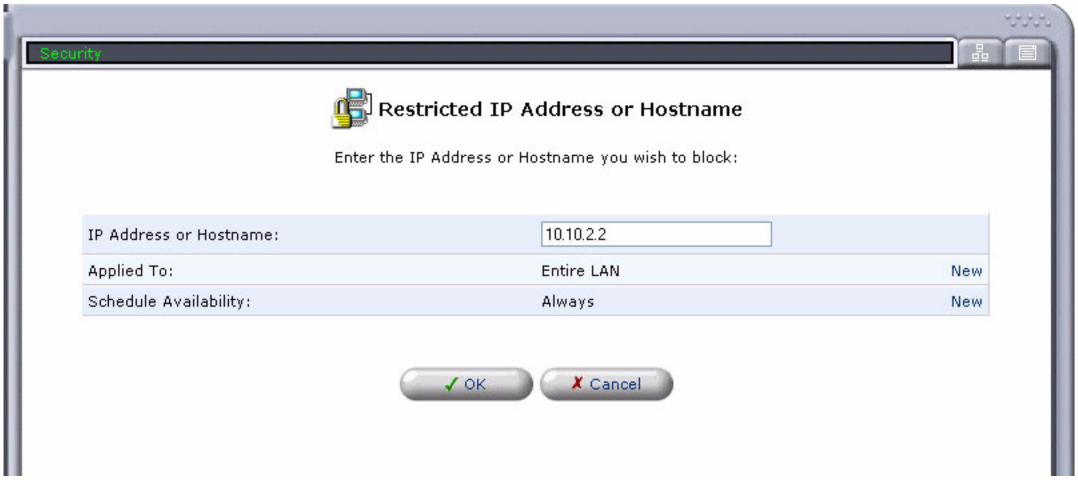


Block access from the LAN to IP Address or Hostname.

IP Address or Hostname	IP Address	Status	Action
New Entry			

Press the **Refresh** button to update the data.

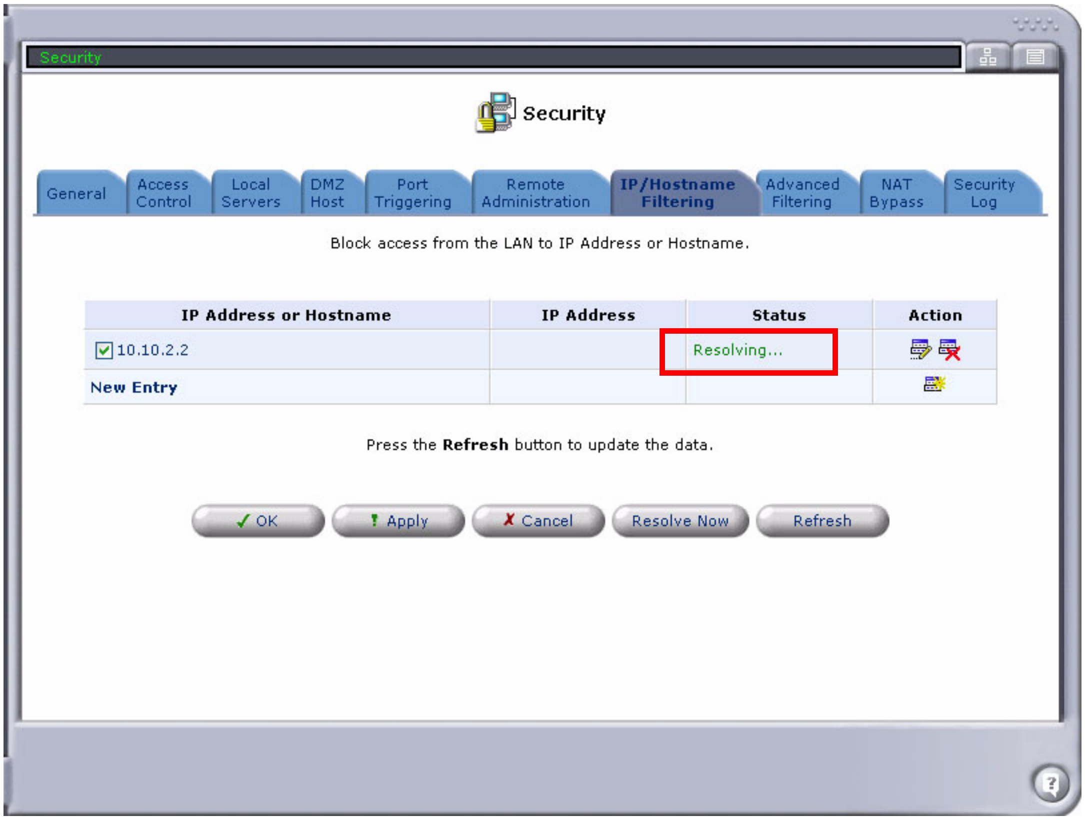
2. Enter an **IP Address** or **Hostname**.
3. **Applied To** - To set this to a setting other than **Entire LAN**, select **New** and define a set of Network Objects that will be restricted. For information on configuring a Network Object, see *Network Objects on page 2-34*.
4. **Scheduled Availability** - To set this to a setting other than **Always**, select **New** and define the schedule. For information on configuring schedule rules, see *Scheduler Rules on page 2-52.*



Enter the IP Address or Hostname you wish to block:

IP Address or Hostname:	10.10.2.2	
Applied To:	Entire LAN	New
Schedule Availability:	Always	New

5. Select **OK** to add the Address to the Restricted list.
6. If the site is successfully located, the **Status** on the **IP/Hostname Filtering** window will transition from **Resolving...** to **Active**. Restricted access to the site can be enabled/disabled at any time with the checkbox next to the address/hostname.



Block access from the LAN to IP Address or Hostname.

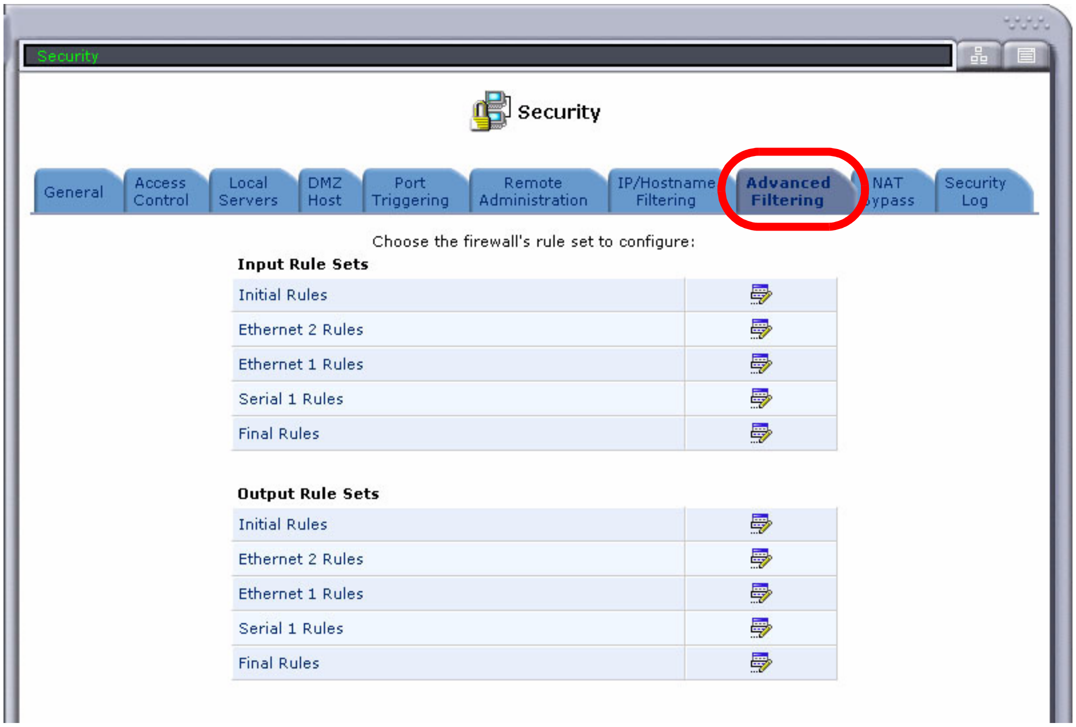
IP Address or Hostname	IP Address	Status	Action
☑ 10.10.2.2		Resolving...	
New Entry			

Press the **Refresh** button to update the data.

Advanced Filtering

Advanced filtering is designed to allow comprehensive control over the firewall’s behavior. You can define specific input and output rules, control the order of logically similar sets of rules, and make a distinction between rules that apply to WAN and LAN network devices. There are two groups of rule sets:

- Input Rule Sets
- Output Rule Sets



Choose the firewall's rule set to configure:

Input Rule Sets

Initial Rules
Ethernet 2 Rules
Ethernet 1 Rules
Serial 1 Rules
Final Rules

Output Rule Sets

Initial Rules
Ethernet 2 Rules
Ethernet 1 Rules
Serial 1 Rules
Final Rules

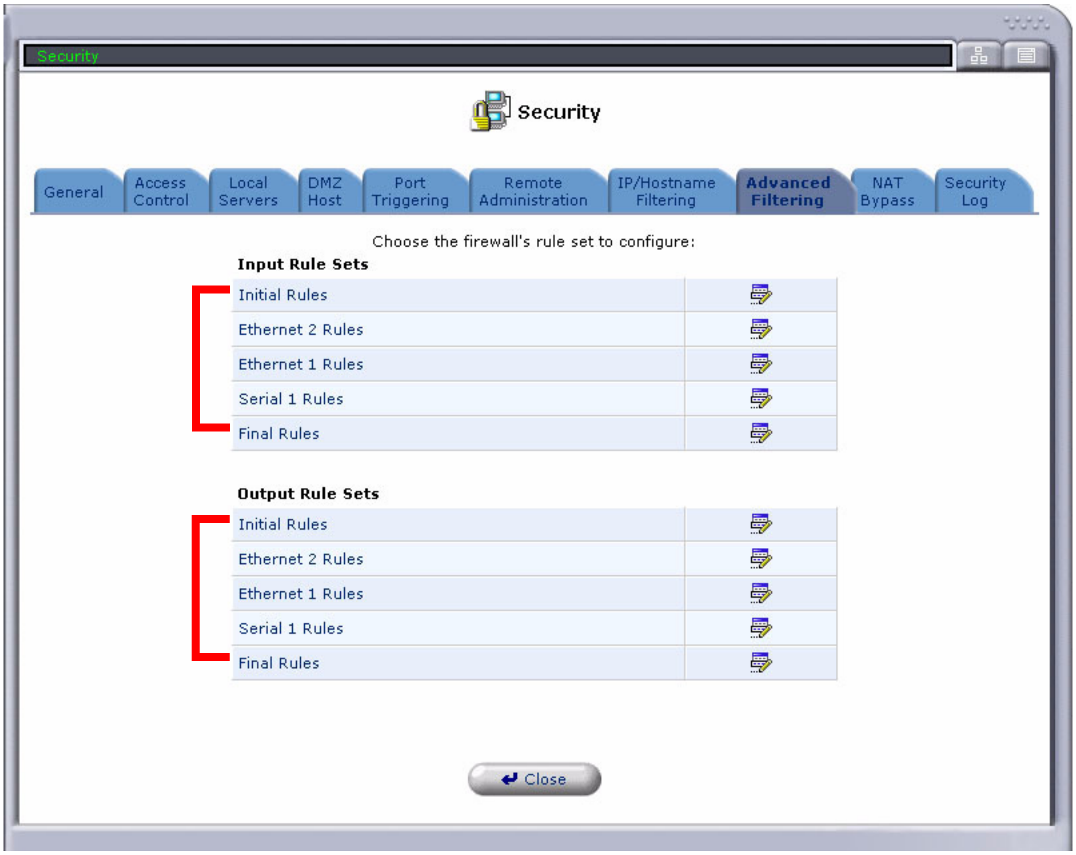
Input and Output Rule Sets

Field	Definition
Initial Rules	Initial rules are applied against packets at any interface before applying any other configured firewall settings. See *Firewall Implementation on page 4-37* for actual sequence.
Ethernet 1 Rules	Interface specific rules are applied against packets at that particular interface immediately after applying the Initial rules. See *Firewall Implementation on page 4-37* for actual sequence. **Note:** The list of connections varies depending on the current connections configured.
Ethernet 2 Rules	
Serial 1 Rules	
Multilink 1 Rules	
Final Rules	Final rules are applied against packets after applying all other configured firewall settings, and before applying the General Security Policy. See *Firewall Implementation on page 4-37* for actual sequence.

Adding an Advanced Filtering Rule

To add a new advanced filtering rule:

1. Select **Security/ Advanced Filtering**.
2. Select the rule set to modify (for example, in the Input Rule Sets, select **Initial Rules**).



Security

Choose the firewall's rule set to configure:

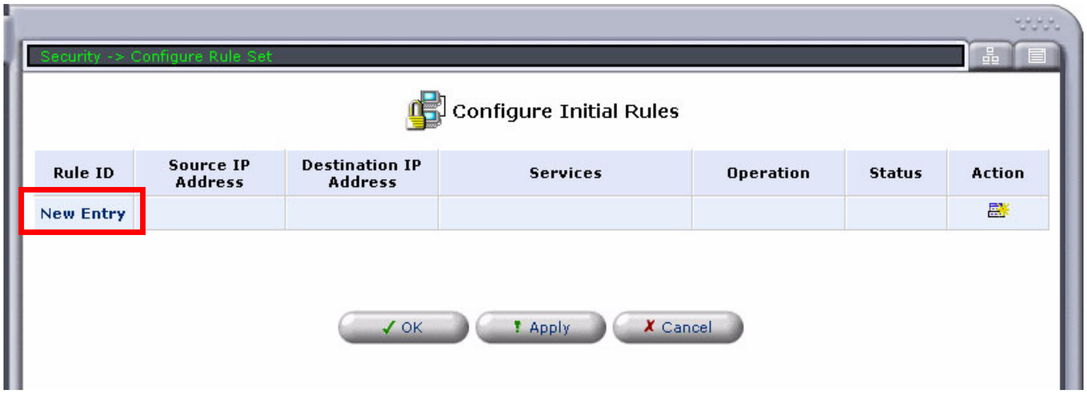
Input Rule Sets

- Initial Rules
- Ethernet 2 Rules
- Ethernet 1 Rules
- Serial 1 Rules
- Final Rules

Output Rule Sets

- Initial Rules
- Ethernet 2 Rules
- Ethernet 1 Rules
- Serial 1 Rules
- Final Rules

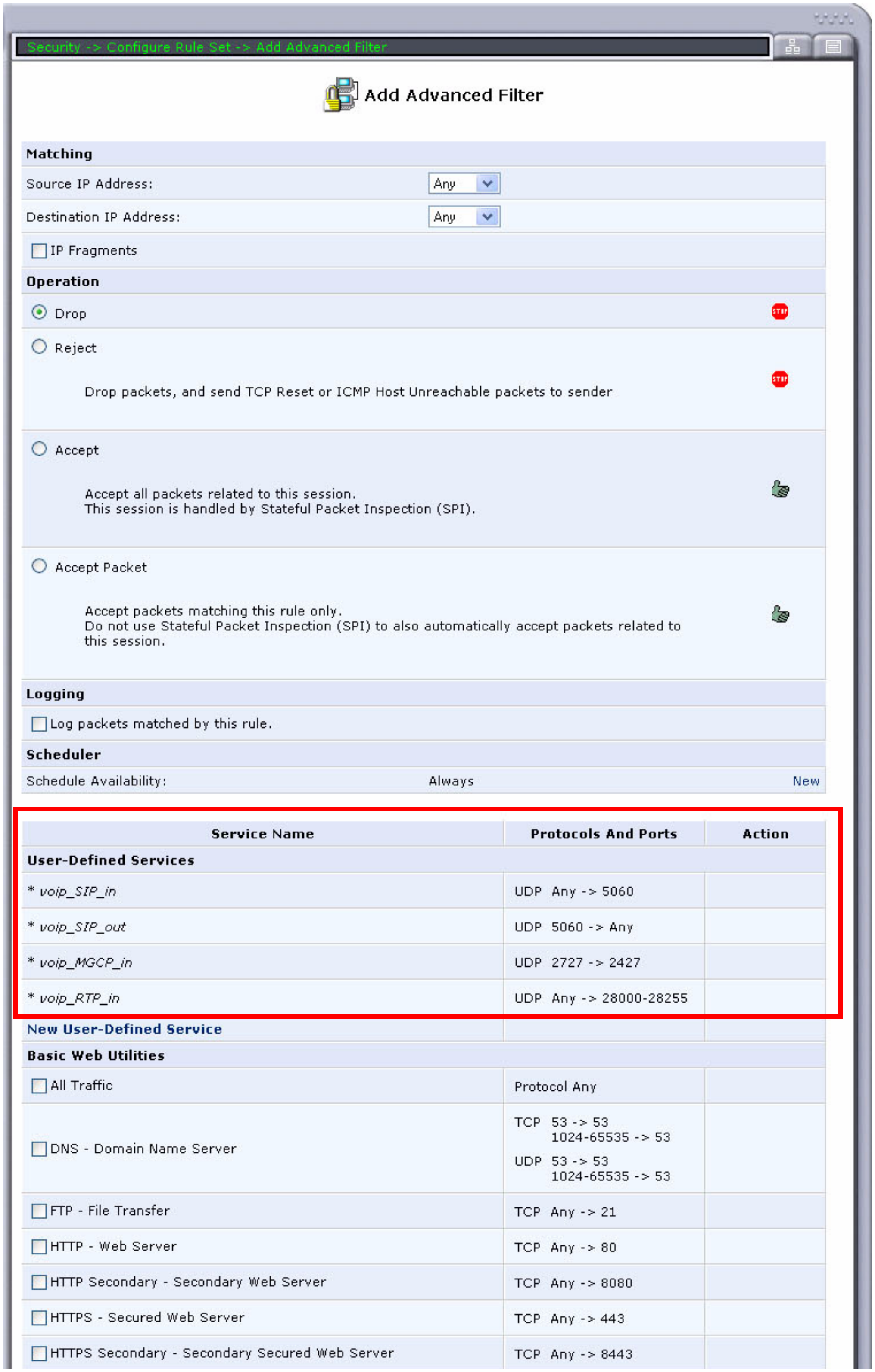
3. On the Configure Initial Rules window, select **New Entry**.



Configure Initial Rules

Rule ID	Source IP Address	Destination IP Address	Services	Operation	Status	Action
New Entry						

4. On the **Add Advanced Filter** window, define the filter (see field definitions below).



Security -> Configure Rule Set -> Add Advanced Filter

Add Advanced Filter

Matching	
Source IP Address:	Any
Destination IP Address:	Any
□ IP Fragments	

Operation

● Drop

○ Reject

Drop packets, and send TCP Reset or ICMP Host Unreachable packets to sender

○ Accept

Accept all packets related to this session.
This session is handled by Stateful Packet Inspection (SPI).

○ Accept Packet

Accept packets matching this rule only.
Do not use Stateful Packet Inspection (SPI) to also automatically accept packets related to this session.

Logging

□ Log packets matched by this rule.

Scheduler

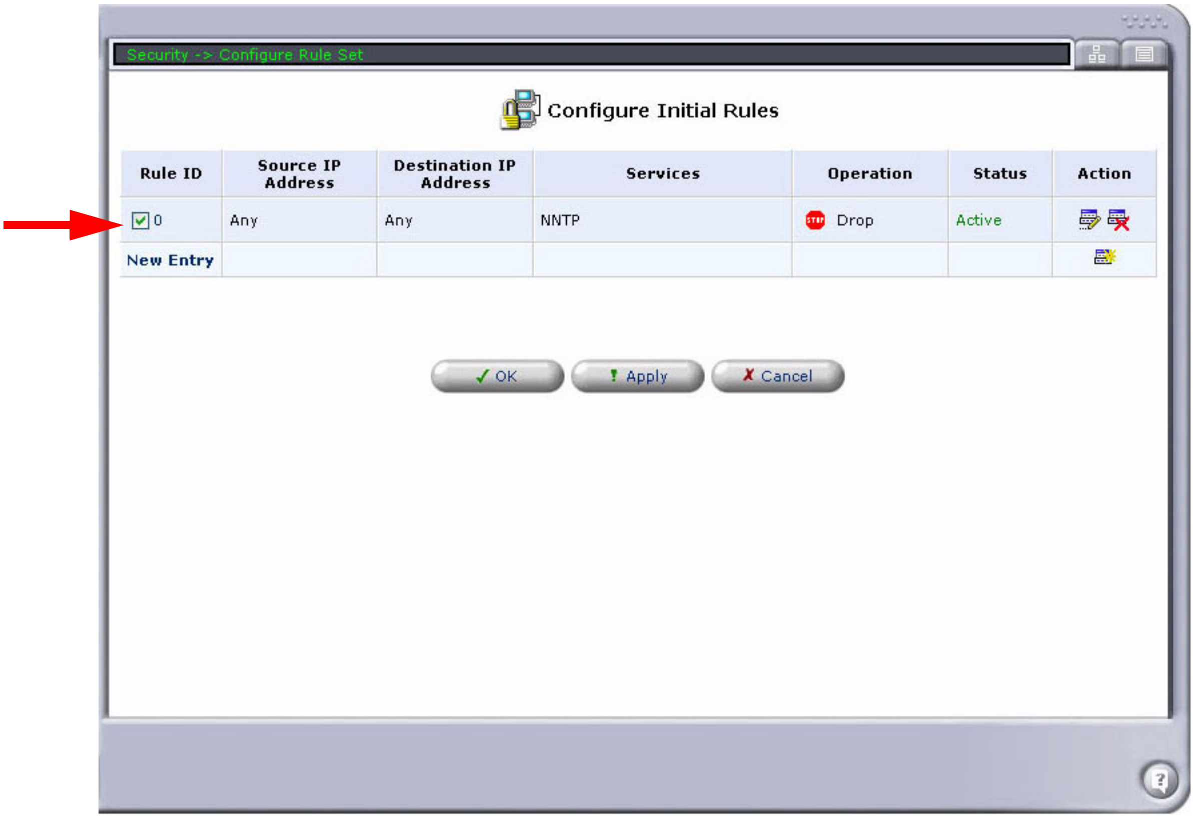
Schedule Availability:	Always	New

Service table is referenced from multiple windows

Service Name	Protocols And Ports	Action
User-Defined Services		
* _voip_SIP_in_	UDP Any -> 5060	
* _voip_SIP_out_	UDP 5060 -> Any	
* _voip_MGCP_in_	UDP 2727 -> 2427	
* _voip_RTP_in_	UDP Any -> 28000-28255	
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	Protocol Any	
□ DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
□ FTP - File Transfer	TCP Any -> 21	
□ HTTP - Web Server	TCP Any -> 80	
□ HTTP Secondary - Secondary Web Server	TCP Any -> 8080	
□ HTTPS - Secured Web Server	TCP Any -> 443	
□ HTTPS Secondary - Secondary Secured Web Server	TCP Any -> 8443	

Field	Definition
Matching - Use this section to define the rule's conditions.	
Source IP Address	The Source IP address of packets sent or received from the LAN computer. This entry is mandatory when defining a rule. **Any** - Apply this rule to any Source IP Address. **Single** - Apply this rule only to this Source IP Address. **Range** - Apply this rule to the following range of Source IP addresses (enter IP address and subnet mask).
Destination IP Address	The Destination IP address of packets sent or received from a Network Object. This entry is mandatory when defining a rule. **Any** - Apply this rule to any Destination IP Address. **Single** - Apply this rule only to this Destination IP Address. **Range** - Apply this rule to the following range of Destination IP addresses (enter IP address and subnet mask).
IP Fragments	This checkbox will allow (checked) or not allow (unchecked) IP fragments.
Operation - Define what action the rule will take by selecting one of the following radio buttons:	
Drop	Deny access to packets that match the source and destination IP addresses defined above.
Reject	Deny access to packets that match the criteria defined, and send an ICMP error or a TCP reset to the origination peer.
Accept	Allow access to packets that match the criteria defined. The data transfer session will be handled using Stateful Packet Inspection (SPI), meaning that other packets matching this rule will be automatically allowed access.
Accept Packet	Allow access to packets that match the criteria defined. The data transfer session will not be handled using SPI, meaning that other packets matching this rule will not be automatically allowed access. This can be useful, for example, when creating rules that allow broadcasting.
Logging	**Log packets matched by this rule.** This checkbox enables/disable logging of these events.
Scheduler	**Scheduled Availability** - To set this to a setting other that Always, select **New** and specify the schedule on the Schedule Rule Edit window. For information on configuring the schedule, see *Scheduler Rules on page 2-52*.
Service Name	Select the services to be applied to this rule. **Note:** The Service table is used by multiple windows; the standard services and the User-Defined services created on any of these windows appear here. For information on creating a **New User-Defined Service**, see *Creating a User-Defined Rule on page 4-10*.

5. Select **OK** to save and enable the rule. The rule is listed in the Configure Initial Rules table. You can disable/enable the rule at any time using the checkbox.

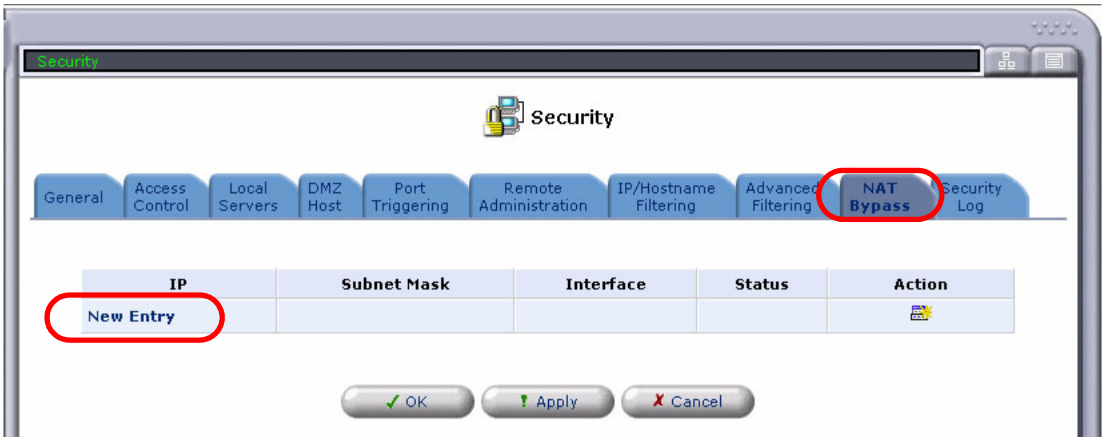


Configure Initial Rules

Rule ID	Source IP Address	Destination IP Address	Services	Operation	Status	Action
☑ 0	Any	Any	NNTP	Drop	Active	
New Entry						

NAT Bypass

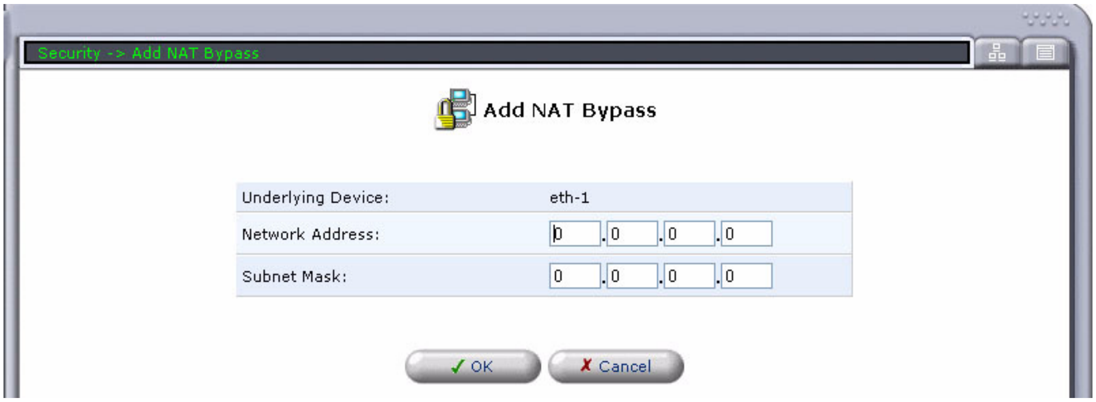
The **Security/NAT Bypass** feature allows network address translation to be bypassed for specific addresses or networks. You can add, modify, and remove NAT bypass rules. The changes take effect immediately. NAT bypass must be set on the WAN network interface.



IP	Subnet Mask	Interface	Status	Action
New Entry				

Adding/Modifying a NAT Bypass Rule

1. Select **Security/ NAT Bypass**.
2. Select the **New Entry** (or select the **edit icon** for an existing entry), and enter/modify the network address and mask:.



Underlying Device:	eth-1
Network Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0

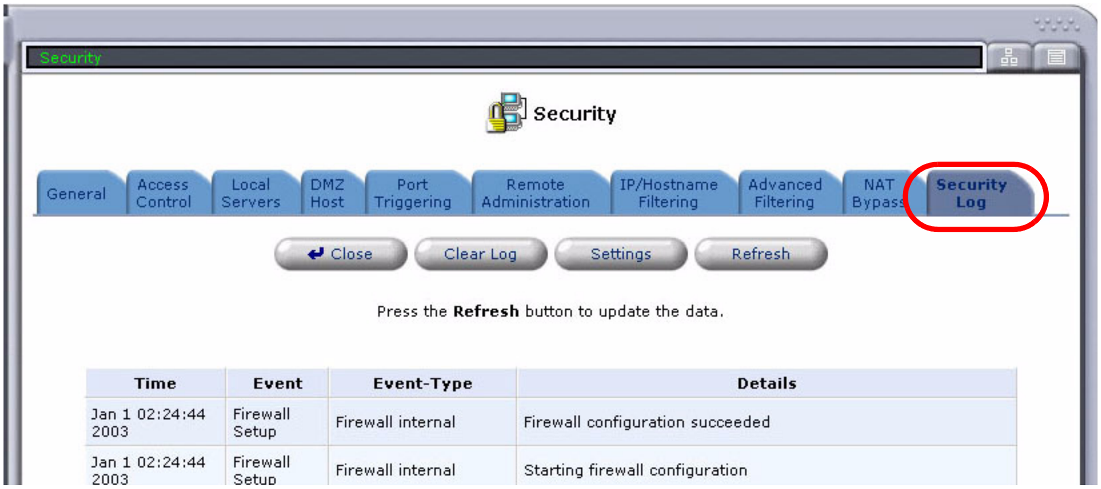
Field	Definition
Underlying Device	Displays the device/connection(s) required for this interface.
Network Address	Enter the IP address to apply NAT bypass to.
Subnet Mask	Enter the subnet mask the applies to the above IP address.

NOTE: Do not enter “0.0.0.0/0.0.0.0” for NAT bypass. This is interpreted as “exclude all networks.” For the same result, it is recommended that you disable NAPT on the WAN interface.

3. Click **OK** to enable the rule. You can disable/enable the rule at any time using the checkbox.

Security Log

The Security Log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface, firewall configuration, and system startup.



Press the **Refresh** button to update the data.

Time	Event	Event-Type	Details
Jan 1 02:24:44 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 02:24:44 2003	Firewall Setup	Firewall internal	Starting firewall configuration

The following are the events and event types that are automatically recorded in the Security Log:

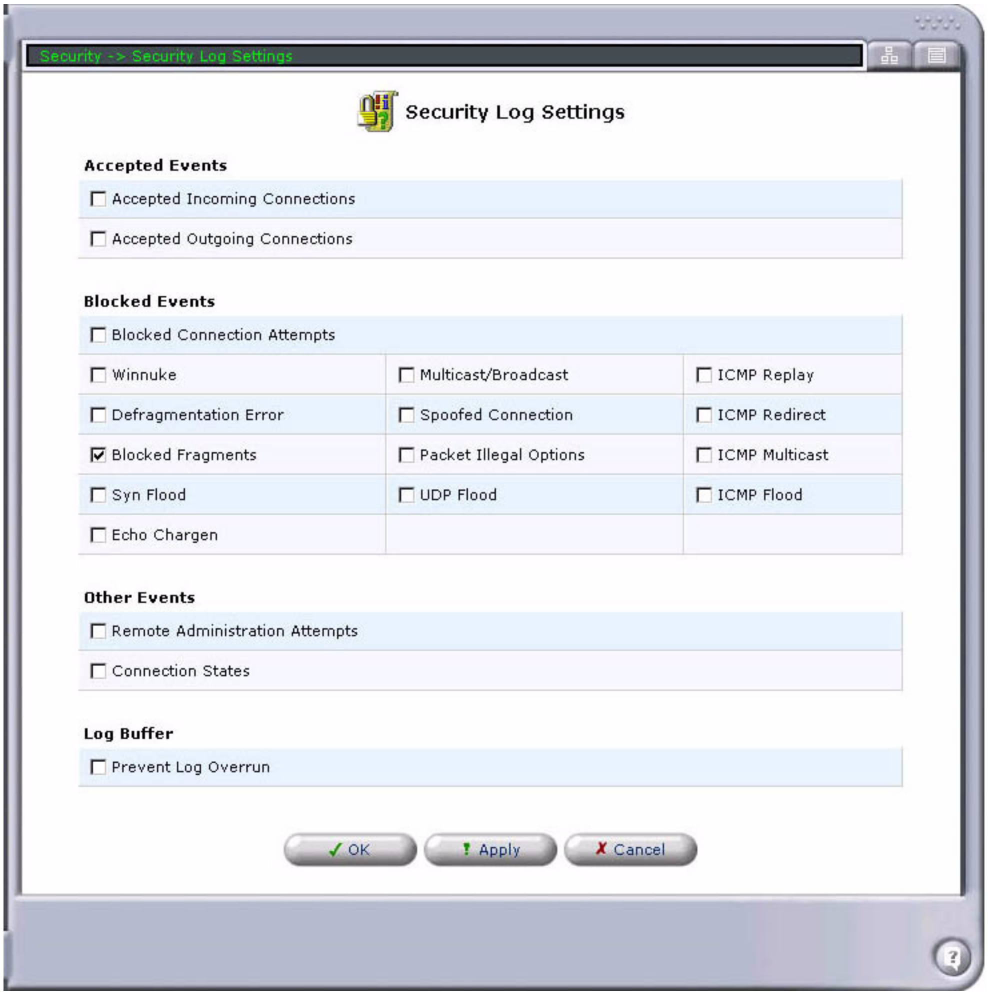
Field	Definition
Inbound/Outbound Traffic	
Connection accepted	Access request complies with the Firewall's security policy.
Accepted - Host probed *	This TCP connection request from a WAN host matches the Firewall's security policy, but the WAN host is not recognized as trusted. The WAN host is being challenged to verify that it is a trusted host.
Accepted - Host trusted *	A reply from a previously challenged WAN host. This client becomes a trusted host.
Accepted - Internal traffic *	All packets are allowed to move freely from one LAN host to another.
Blocked - Policy violation	This access request violates the Firewall's security policy.
Blocked - IP Fragment	If the Firewall is configured to block all IP fragments, this message is recorded for every blocked fragmented packet.
Blocked - IP Source-Routes	This message is recorded whenever a packet is blocked due to a Source Route (either strict or loose) option set in its IP header.
Blocked - State-table error	The Firewall encountered an error during State-table lookup or manipulation. Packet was blocked.
Firewall Setup	Aborting configuration Configuration complete
WBM Login	Authentication Success Authentication Failure
Telnet Login	Authentication Success Authentication Failure
System Up/Down	The system is going DOWN for reboot The system is UP!

* Appears only with regard to inbound traffic.

Changing the Security Log Settings

To change the settings for the Security Log:

1. Select **Security/ Security Log**.
2. Select **Settings**.
3. Modify the settings as necessary (see the following table), then select **OK**.



Accepted Events

☐ Accepted Incoming Connections
☐ Accepted Outgoing Connections

Blocked Events

☐ Blocked Connection Attempts

☐ Winnuke	☐ Multicast/Broadcast	☐ ICMP Replay
☐ Defragmentation Error	☐ Spoofed Connection	☐ ICMP Redirect
☑ Blocked Fragments	☐ Packet Illegal Options	☐ ICMP Multicast
☐ Syn Flood	☐ UDP Flood	☐ ICMP Flood
☐ Echo Chargen		

Other Events

☐ Remote Administration Attempts
☐ Connection States

Log Buffer

☐ Prevent Log Overrun

Security Log Settings

Field	Definition
Accepted Events	
Accepted Incoming Connections	Sessions originated from the Internet that have been allowed by the firewall.
Accepted Outgoing Connections	Sessions originated from the network that have been allowed by the firewall.
Blocked Events	
Blocked Connection Attempts	Sessions that have been blocked by the firewall.
Winnuke	Detection of the Winnuke DOS attack.
Defragmentation Error	Detection of fragmented packets that cannot be properly reassembled.
Blocked Fragments	Detection of fragmented packets when Block IP Fragments is enabled.
Syn Flood	Detection of the Syn Flood DOS attack.
Echo Cargen	Detection of the Echo or Chargen DOS attacks.
Multicast/Broadcast	Detection of the multicast or broadcast packets arriving at the WAN interface.
Spoofed Connection	Detection of IP address spoofing attacks.
Packet Illegal Options	Detection of IP packets with disallowed IP options: lsrr, ssrr, rr, timestamp, or error options.
UDP Flood	Detection of a UDP Flood attack.
ICMP Replay	Detection of an ICMP Replay DOS attack.
ICMP Redirect	Detection of improper ICMP redirect messages from the WAN.
ICMP Multicast	Detection of multicast ICMP packets, such as a ping to a subnet broadcast address.
ICMP Flood	Detection of an ICMP flood DOS attack.
Other Events	
Remote Administration Attempts	Management sessions established to the Adit.
Connection States	Session connection state detail.
Log Buffer	
Prevent Log Overrun	Stop logging firewall detail when the log is full. This prevents loosing early log entries, but will drop the later log entries.

Firewall Implementation

The Adit provides very powerful NAT and firewall capabilities. This section provides some of the underlying implementation details so that users who are familiar with the low-level action of firewalls will know what behaviors to expect from the Adit. Users who do not need this level of detail can skip this section.

Network Connection Configuration

The Network Connection setup screens contain three configuration items for each IP interface that influence the NAT and firewall behavior of the Adit. These include the **Network Type**, **Routing Mode**, and **Internet Connection Firewall** settings, described below.

Network Type

Normally the user does not need to change the network type from the default setting applied when the network connection is created. The effects of each setting are as follows:

LAN

A network connection designated as type LAN is used for private LAN hosts. This is usually the local network containing hosts that are directly managed by the local administrator. From the firewall perspective, hosts on the LAN connections are considered inherently trusted, unless designated otherwise by the administrator. When NAPT routing mode is enabled on other WAN network connections, hosts that are in the directly connected subnets of any LAN network connection will have NAPT applied against sessions that are initiated from the LAN network toward the WAN network.

WAN

A network connection designated as type WAN is used for the interface that provides a path to the Internet. From the firewall perspective, hosts on the WAN interfaces are considered inherently untrusted, unless designated otherwise by the administrator. WAN interfaces are typically secured by enabling the Internet Connection Firewall and often using NAPT routing mode if connected to the Internet.

DMZ

A network connection designated as type DMZ is used for an interface that contains servers that provide public access. Packets between a DMZ network interface and a WAN network interface are passed by default, unless explicitly blocked by user configured rules (see the processing sequence tables in *Firewall Processing Sequence on page 4-39*). This designation, with its inherent insecurity, should not typically be needed by most users. There are other ways to expose servers to the public hosts that are more secure and better suited to mixing both servers and private hosts on the same interface.

Routing Mode

The routing mode determines whether NAPT (Network Address Port Translation) is applied to sessions that are created through this interface.

NAPT

When set to NAPT mode, dynamic sessions initiated by hosts in the LAN subnets to hosts reachable through this interface will have NAPT applied to them. For these sessions, the local IP address will be translated to the WAN IP address of the Adit, and the local port will be retained if possible. If there is already a session using this combination of translated IP address and port, then a dynamically selected port will be assigned to the session and the port will be translated as well.

It should be noted that even with NAPT enabled, sessions initiated from public hosts on the WAN interfaces to the private local addresses are allowed unless the firewall is enabled and configured to block these connection attempts. This behavior differs from that of some typical routers.

Route

When set to Route mode, no NAPT behavior is applied to dynamic sessions initiated by hosts in the LAN subnets. It should be noted, however, that NAPT, can still be applied to sessions initiated from public hosts on the WAN if they are directed to the Adit's own IP address and there is a matching Local Server or DMZ Host configuration.

Internet Connection Firewall

The Internet Connection Firewall setting enables or disables firewall processing on the interface. If enabled, all of the packets arriving or departing through this interface are examined against the configured firewall policies. If not enabled, the packets pass though this interface without examination.

In the most typical configuration of the Adit, providing Internet access to hosts on a private LAN, both NAPT routing mode and firewall should be enabled on the WAN interface, and the firewall can be disabled on the LAN interface. In such a configuration, packets are transmitted and received freely at the LAN interface, but are scrutinized as they enter or leave through the WAN interface.

If NAPT routing mode is configured on the interface, the dynamic NAPT behavior is applied whether or not the firewall is enabled on the interface. It should be noted that, unlike some routers, even if NAPT is enabled, sessions initiated from public hosts on the WAN interfaces to the private local addresses are allowed unless the firewall is enabled and configured to block these connection attempts.

For the reasons above, it is highly recommended that the user enable the firewall when using NAPT on WAN interfaces.

Firewall Processing Sequence

This section details the sequence of processing that is used by the firewall when examining packets. This detail can help an experienced user better understand the order of application of each of the various security settings. The order processing is separately described for both inbound processing and outbound processing at an interface that has firewall and/or NAPT enabled. Note that if the interface is set for route mode with the firewall disabled, none of the packets are examined or translated either inbound or outbound at that interface boundary.

Inbound Firewall Processing

The following table describes the sequence of examination of packets arriving at the interface. This firewall processing is applied after the layer 2 driver and before passing the inbound packet up to the IP stack. If the action for matching packets at a particular step is described as PASS, no further firewall examination is applied and the packet is passed up to the IP stack. If the action is described as DROP, the packet is dropped and not passed up to the stack. Packets that do not match the criteria at that step continue processing at the next step. Packets that are passed by the firewall and require NAPT translation are translated before passing the packet up to the IP stack.

Step	Test	Action
1	Insecure IP options: loose source route, strict source route, record route, time stamp, or invalid IP option	DROP
2	Invalid IP fragments	DROP
3	Match existing sessions: this matches ongoing sessions and applies NAPT where appropriate.	PASS
4	Packets generated by the firewall itself; e.g. TCP RST packets.	PASS
5	User configured Advanced Filtering/Input Rule Sets/Initial Rules	as per filter
6	User configured Advanced Filtering/Input Rule Sets/Interface Specific Rules	as per filter
7	Standard Inbound Security: - ICMP to broadcast address - ICMP Redirect from the WAN - Source of destination IP address in loopback subnet - Source address from external host is Adit IP address - IP address spoofed (source address from one interface in other interface subnet) - Source IP address is broadcast, multicast, or experimental - Echo, Chargen, Snork, or Quote DoS (src port 7, 17, or 19; or src & dst port 135)	DROP
8	User configured Local Server	PASS (NAPT)
9	To Adit IP address & user configured Remote Management	PASS
10	SIP and RTP local ports	PASS
11	Active IPSEC tunnel	PASS
12	TCP Auth/Ident protocol (to TCP port 113)	DROP
13	To Adit IP address & user configured DMZ Host	PASS (NAPT)
14	Packet between DMZ interface and WAN interface	PASS
15	User configured Advanced Filtering/Input Rule Sets/Final Rules	as per filter
last	Take default action based on user configured General Security Policy: Maximum Security Typical Security Minimum Security	 DROP DROP PASS

Outbound Firewall Processing

The following table describes the sequence of examination of packets departing from the interface. This firewall processing is applied after the IP stack and before passing the outbound packet down to the layer 2 driver. If the action for matching packets at a particular step is described as PASS, no further firewall examination is applied and the packet is passed down to the driver. If the action is described as DROP, the packet is dropped and not passed down to the driver. Packets that do not match the criteria at that step continue processing at the next step. Packets that are passed by the firewall and require NAPT translation are translated before passing the packet down to the driver.

Step	Test	Action
1	Insecure IP options: loose source route, strict source route, record route, time stamp, or invalid IP option	DROP
2	Invalid IP fragments	DROP
3	Match existing sessions: this matches ongoing sessions and applies NAPT where appropriate.	PASS
4	Packets generated by the firewall itself; e.g. TCP RST packets.	PASS
5	User configured Advanced Filtering/Output Rule Sets/Initial Rules	as per filter
6	User configured Advanced Filtering/Output Rule Sets/Interface Specific Rules	as per filter
10	SIP and RTP local ports	PASS
11	User configured Access Control (based on source)	DROP
12	User configured IP/Hostname Filtering (based on destination)	DROP
13	TCP Auth requests (TCP source port 113)	PASS
14	Packet between DMZ interface and WAN interface	PASS
15	User configured Advanced Filtering/Output Rule Sets/Final Rules	as per filter
last	Take default action based on user configured General Security Policy:	
	Maximum Security	DROP
	Typical Security	PASS
	Minimum Security	PASS

CHAPTER 5

System Monitoring

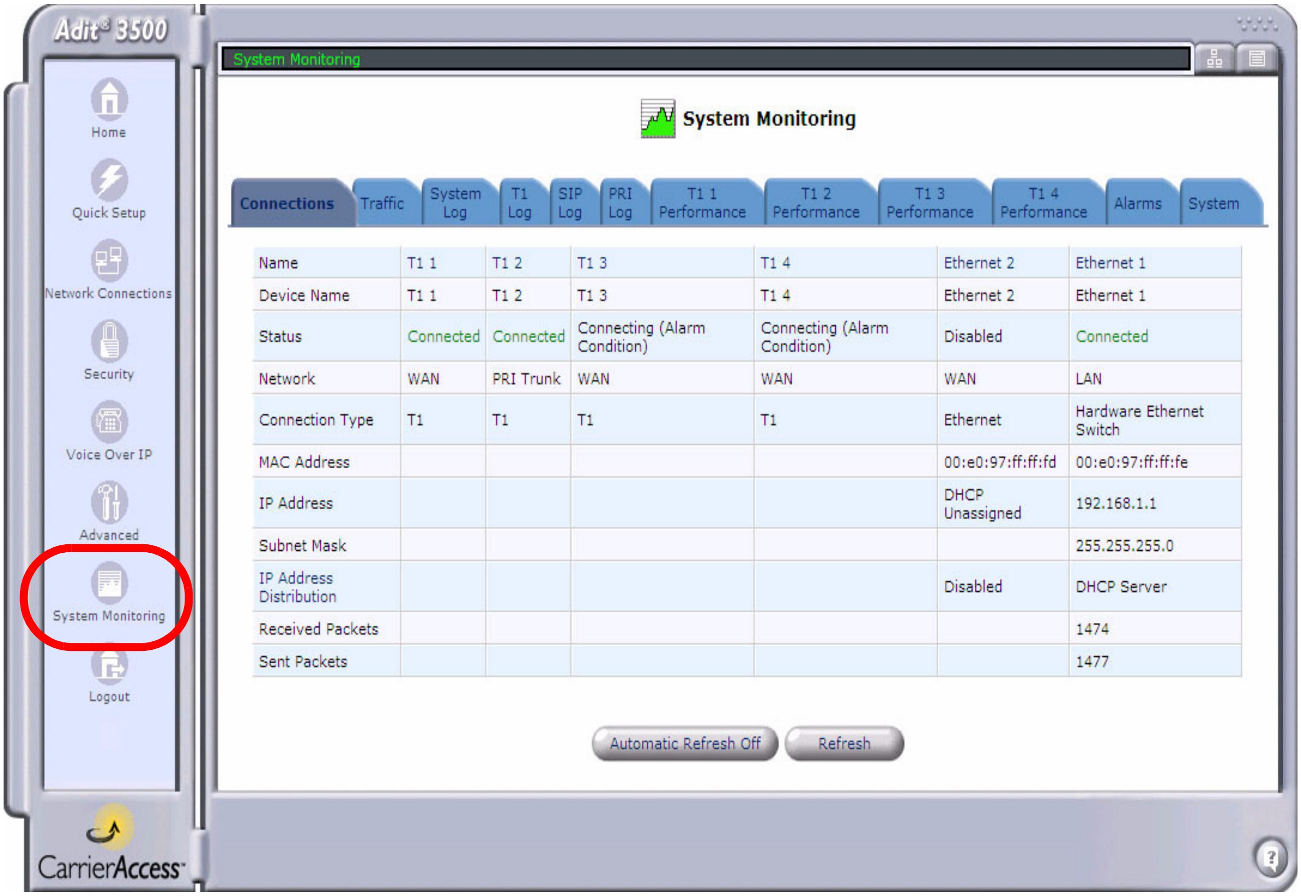
In this Chapter

- Overview
- Connections
- Traffic
- System Log
- T1 Log (Adit 3000 Only)
- SIP Log
- PRI Log
- T1 Performance (Adit 3000 Only)
- Alarms
- System

Overview

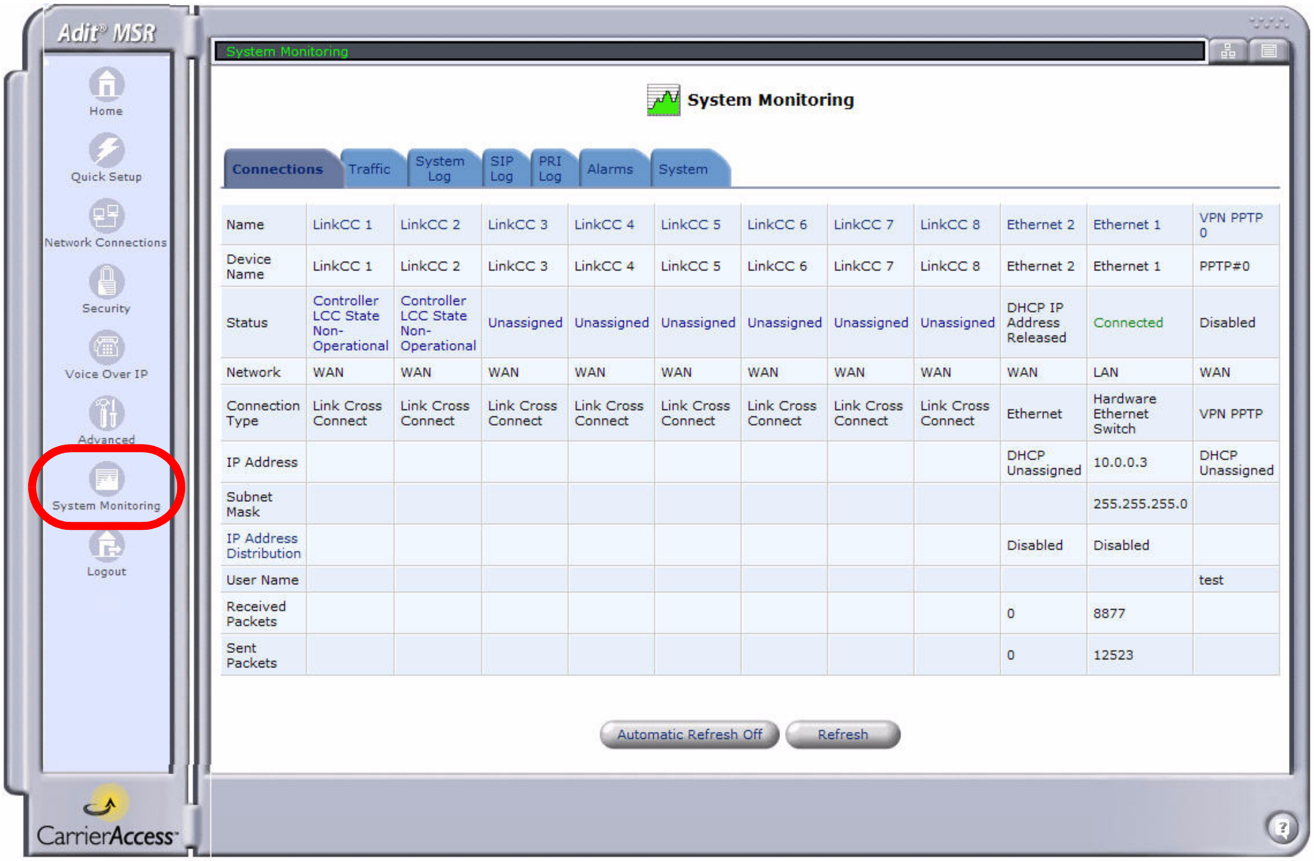
The System Monitoring window displays information that can be used for monitoring and troubleshooting the system. As shown in the following figures, the types of information provided through the System Monitoring window differs between the Adit 3000 and Adit MSR.

Adit 3500



Name	T1 1	T1 2	T1 3	T1 4	Ethernet 2	Ethernet 1
Device Name	T1 1	T1 2	T1 3	T1 4	Ethernet 2	Ethernet 1
Status	Connected	Connected	Connecting (Alarm Condition)	Connecting (Alarm Condition)	Disabled	Connected
Network	WAN	PRI Trunk	WAN	WAN	WAN	LAN
Connection Type	T1	T1	T1	T1	Ethernet	Hardware Ethernet Switch
MAC Address					00:e0:97:ff:ff:fd	00:e0:97:ff:ff:fe
IP Address					DHCP Unassigned	192.168.1.1
Subnet Mask						255.255.255.0
IP Address Distribution					Disabled	DHCP Server
Received Packets						1474
Sent Packets						1477

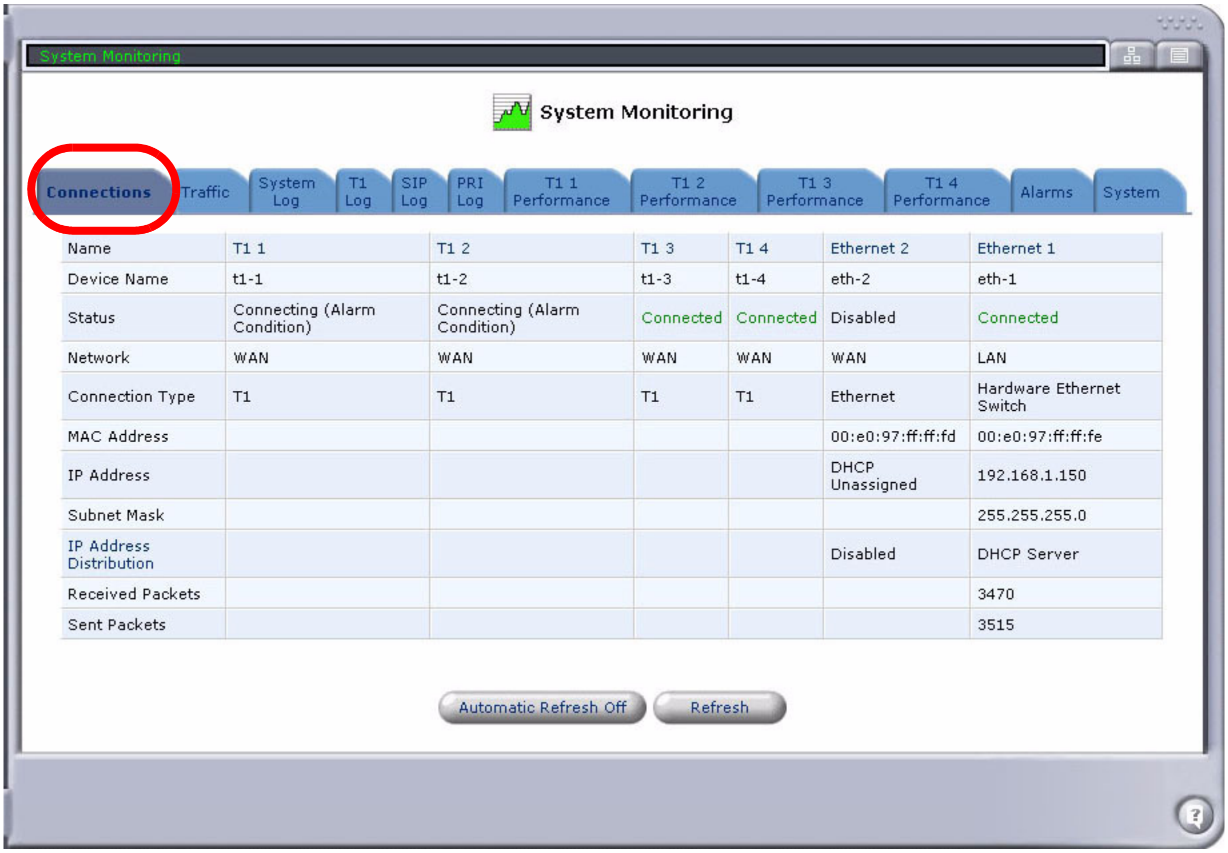
Adit MSR



Name	LinkCC 1	LinkCC 2	LinkCC 3	LinkCC 4	LinkCC 5	LinkCC 6	LinkCC 7	LinkCC 8	Ethernet 2	Ethernet 1	VPN PPTP 0
Device Name	LinkCC 1	LinkCC 2	LinkCC 3	LinkCC 4	LinkCC 5	LinkCC 6	LinkCC 7	LinkCC 8	Ethernet 2	Ethernet 1	PPTP#0
Status	Controller LCC State Non-Operational	Controller LCC State Non-Operational	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	Unassigned	DHCP IP Address Released	Connected	Disabled
Network	WAN	WAN	WAN	WAN	WAN	WAN	WAN	WAN	WAN	LAN	WAN
Connection Type	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Link Cross Connect	Ethernet	Hardware Ethernet Switch	VPN PPTP
IP Address									DHCP Unassigned	10.0.0.3	DHCP Unassigned
Subnet Mask										255.255.255.0	
IP Address Distribution									Disabled	Disabled	
User Name											test
Received Packets									0	8877	
Sent Packets									0	12523	

Connections

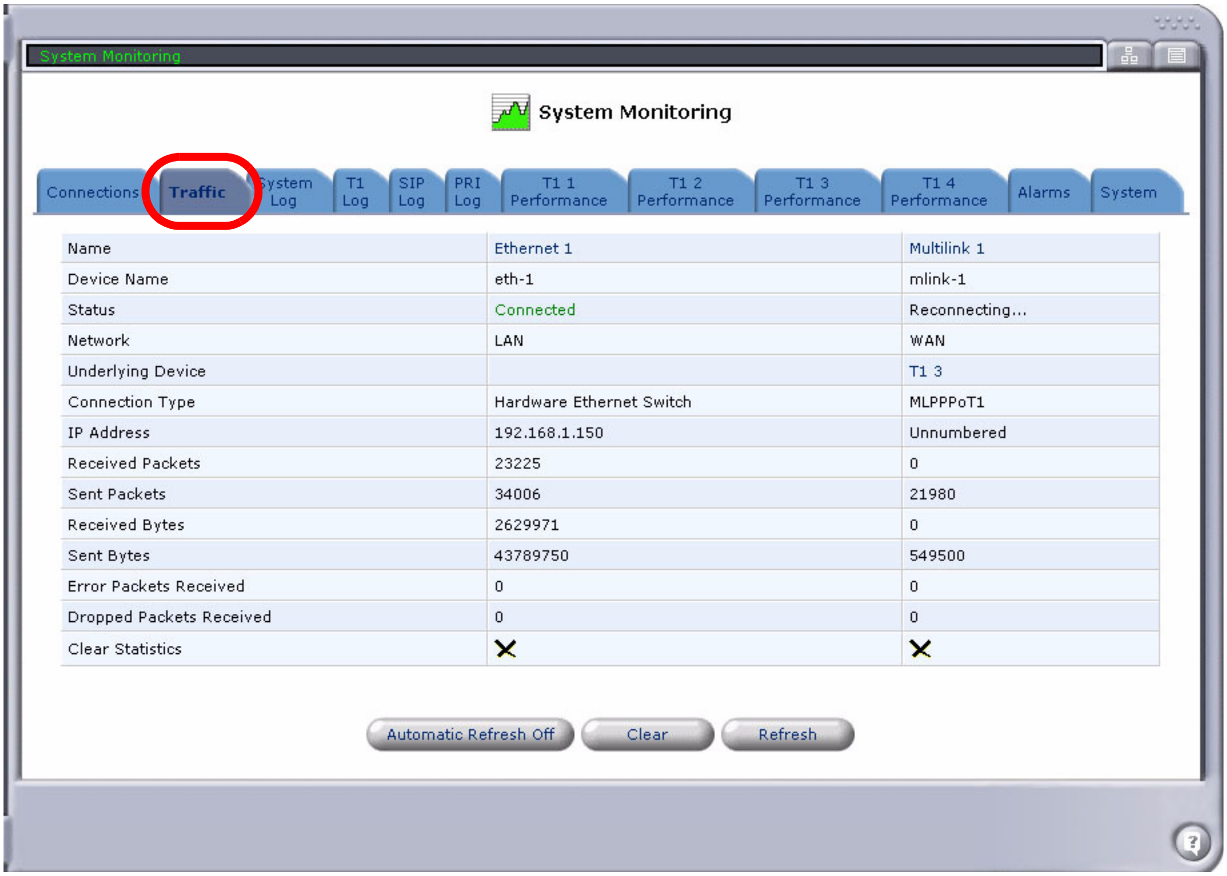
The **Connections** tab displays all the connections, their status, and other information specific to each connection.



Name	T1 1	T1 2	T1 3	T1 4	Ethernet 2	Ethernet 1
Device Name	t1-1	t1-2	t1-3	t1-4	eth-2	eth-1
Status	Connecting (Alarm Condition)	Connecting (Alarm Condition)	Connected	Connected	Disabled	Connected
Network	WAN	WAN	WAN	WAN	WAN	LAN
Connection Type	T1	T1	T1	T1	Ethernet	Hardware Ethernet Switch
MAC Address					00:e0:97:ff:ff:fd	00:e0:97:ff:ff:fe
IP Address					DHCP Unassigned	192.168.1.150
Subnet Mask						255.255.255.0
IP Address Distribution					Disabled	DHCP Server
Received Packets						3470
Sent Packets						3515

Traffic

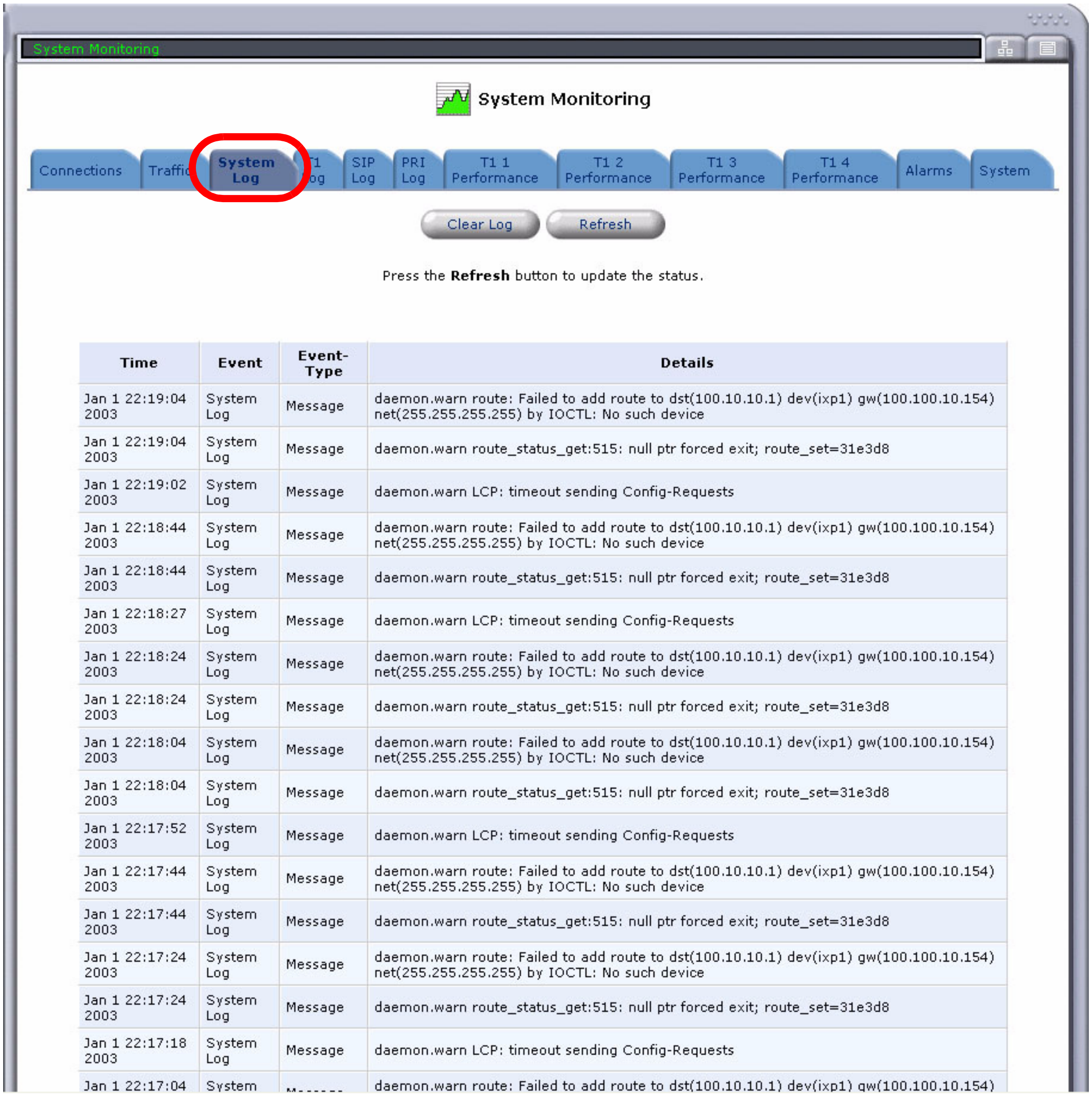
The Adit is constantly monitoring traffic within the local network and between the local network and the Internet. Select the **Traffic** tab to view the current statistical information about data received from and transmitted to the Internet (WAN), and about data received from and transmitted to computers in the local network (LAN).



Name	Ethernet 1	Multilink 1
Device Name	eth-1	mlink-1
Status	Connected	Reconnecting...
Network	LAN	WAN
Underlying Device		T1 3
Connection Type	Hardware Ethernet Switch	MLPPPoT1
IP Address	192.168.1.150	Unnumbered
Received Packets	23225	0
Sent Packets	34006	21980
Received Bytes	2629971	0
Sent Bytes	43789750	549500
Error Packets Received	0	0
Dropped Packets Received	0	0
Clear Statistics	✕	✕

System Log

The **System Log** displays a list of the most recent activity that has taken place on the network.

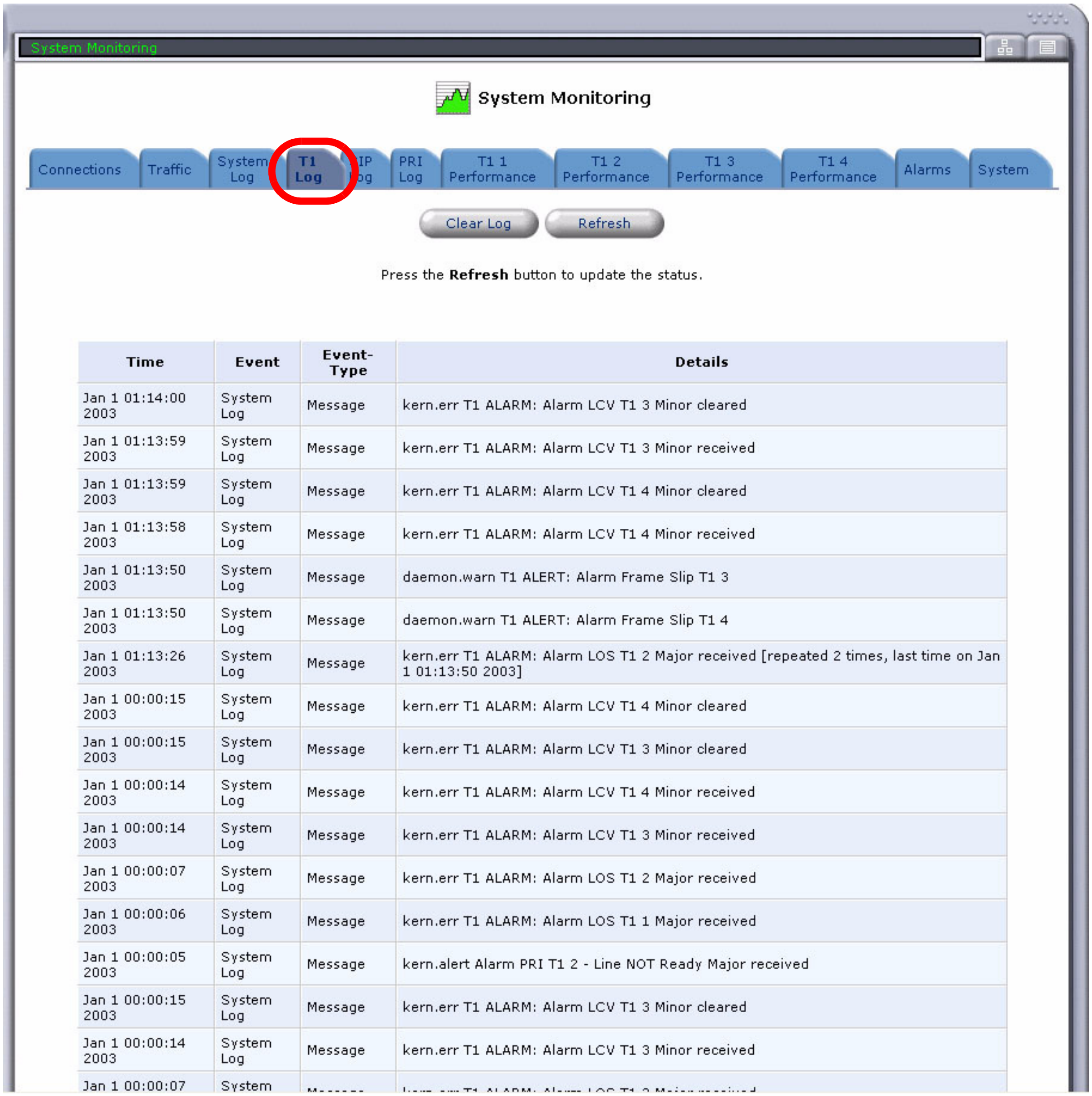


Press the **Refresh** button to update the status.

Time	Event	Event-Type	Details
Jan 1 22:19:04 2003	System Log	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154) net(255.255.255.255) by IOCTL: No such device
Jan 1 22:19:04 2003	System Log	Message	daemon.warn route_status_get:515: null ptr forced exit; route_set=31e3d8
Jan 1 22:19:02 2003	System Log	Message	daemon.warn LCP: timeout sending Config-Requests
Jan 1 22:18:44 2003	System Log	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154) net(255.255.255.255) by IOCTL: No such device
Jan 1 22:18:44 2003	System Log	Message	daemon.warn route_status_get:515: null ptr forced exit; route_set=31e3d8
Jan 1 22:18:27 2003	System Log	Message	daemon.warn LCP: timeout sending Config-Requests
Jan 1 22:18:24 2003	System Log	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154) net(255.255.255.255) by IOCTL: No such device
Jan 1 22:18:24 2003	System Log	Message	daemon.warn route_status_get:515: null ptr forced exit; route_set=31e3d8
Jan 1 22:18:04 2003	System Log	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154) net(255.255.255.255) by IOCTL: No such device
Jan 1 22:18:04 2003	System Log	Message	daemon.warn route_status_get:515: null ptr forced exit; route_set=31e3d8
Jan 1 22:17:52 2003	System Log	Message	daemon.warn LCP: timeout sending Config-Requests
Jan 1 22:17:44 2003	System Log	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154) net(255.255.255.255) by IOCTL: No such device
Jan 1 22:17:44 2003	System Log	Message	daemon.warn route_status_get:515: null ptr forced exit; route_set=31e3d8
Jan 1 22:17:24 2003	System Log	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154) net(255.255.255.255) by IOCTL: No such device
Jan 1 22:17:24 2003	System Log	Message	daemon.warn route_status_get:515: null ptr forced exit; route_set=31e3d8
Jan 1 22:17:18 2003	System Log	Message	daemon.warn LCP: timeout sending Config-Requests
Jan 1 22:17:04	System	Message	daemon.warn route: Failed to add route to dst(100.10.10.1) dev(ixp1) gw(100.100.10.154)

T1 Log (Adit 3000 Only)

The **T1 Log** displays all T1 related alarms and events for the Adit 3000.

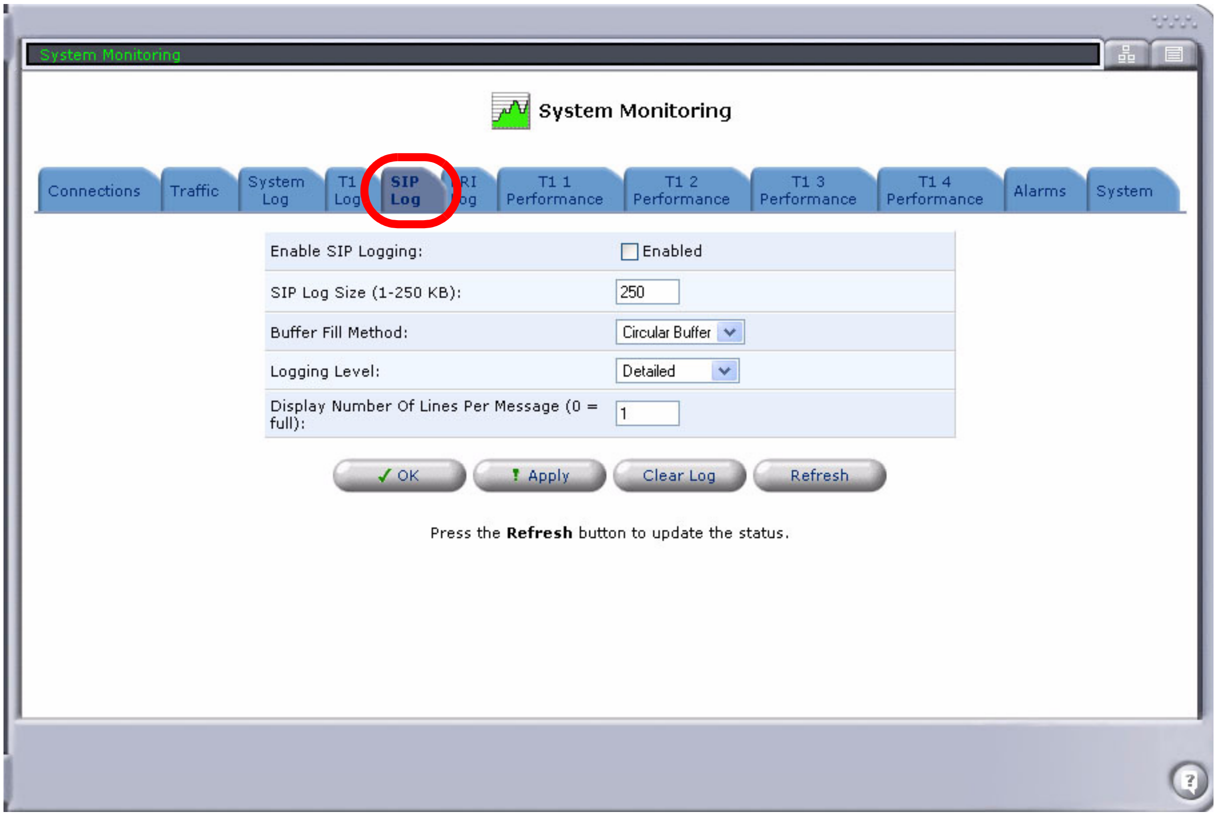


Press the **Refresh** button to update the status.

Time	Event	Event-Type	Details
Jan 1 01:14:00 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 3 Minor cleared
Jan 1 01:13:59 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 3 Minor received
Jan 1 01:13:59 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 4 Minor cleared
Jan 1 01:13:58 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 4 Minor received
Jan 1 01:13:50 2003	System Log	Message	daemon.warn T1 ALERT: Alarm Frame Slip T1 3
Jan 1 01:13:50 2003	System Log	Message	daemon.warn T1 ALERT: Alarm Frame Slip T1 4
Jan 1 01:13:26 2003	System Log	Message	kern.err T1 ALARM: Alarm LOS T1 2 Major received [repeated 2 times, last time on Jan 1 01:13:50 2003]
Jan 1 00:00:15 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 4 Minor cleared
Jan 1 00:00:15 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 3 Minor cleared
Jan 1 00:00:14 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 4 Minor received
Jan 1 00:00:14 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 3 Minor received
Jan 1 00:00:07 2003	System Log	Message	kern.err T1 ALARM: Alarm LOS T1 2 Major received
Jan 1 00:00:06 2003	System Log	Message	kern.err T1 ALARM: Alarm LOS T1 1 Major received
Jan 1 00:00:05 2003	System Log	Message	kern.alert Alarm PRI T1 2 - Line NOT Ready Major received
Jan 1 00:00:15 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 3 Minor cleared
Jan 1 00:00:14 2003	System Log	Message	kern.err T1 ALARM: Alarm LCV T1 3 Minor received
Jan 1 00:00:07	System		

SIP Log

The **SIP Log** displays all SIP related alarms and events.



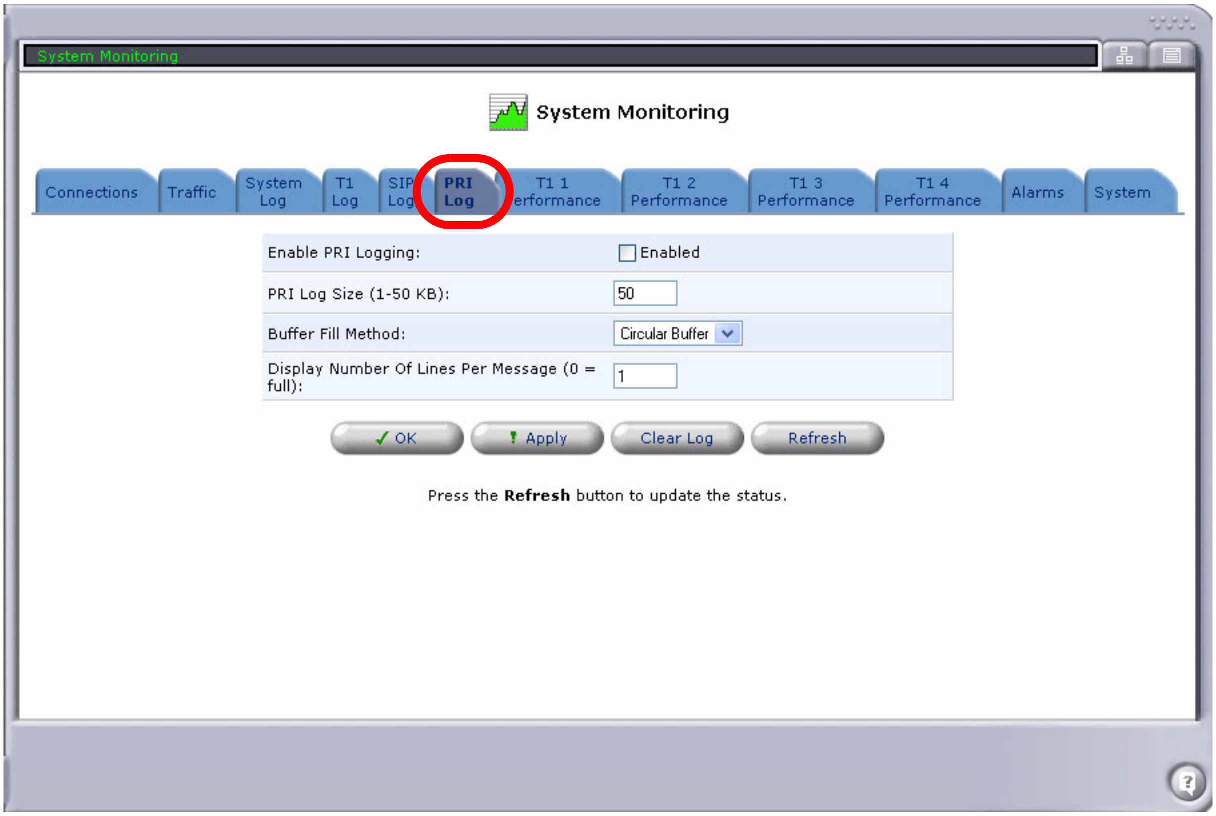
Enable SIP Logging:	□ Enabled
SIP Log Size (1-250 KB):	250
Buffer Fill Method:	Circular Buffer
Logging Level:	Detailed
Display Number Of Lines Per Message (0 = full):	1

Press the **Refresh** button to update the status.

Field	Definition
Enable SIP Logging	Use this checkbox to enable (check) or disable (unchecked) SIP logging.
SIP Log Size	Configure the SIP log size. Range is 1 - 250KB, with a default of 250KB.
Buffer Fill Method	Define the method of loading the buffer. **Circular Buffer** - the buffer will store a continuous stream of data by starting again at the beginning of the buffer after reaching the end. Default. **Fill Until Full** - the buffer will fill until it is full. The user will have to clear the log manually.
Logging Level	Defines how the logs are displayed. **Detailed** - Display detailed information of the log. **Non-Detailed** - Display brief information of the log.
Display Number of Lines Per Message	Defines the number of lines per message. 0 = full

PRI Log

The **PRI Log** displays all PRI related alarms and events.



Enable PRI Logging: □ Enabled

PRI Log Size (1-50 KB): 50

Buffer Fill Method: Circular Buffer

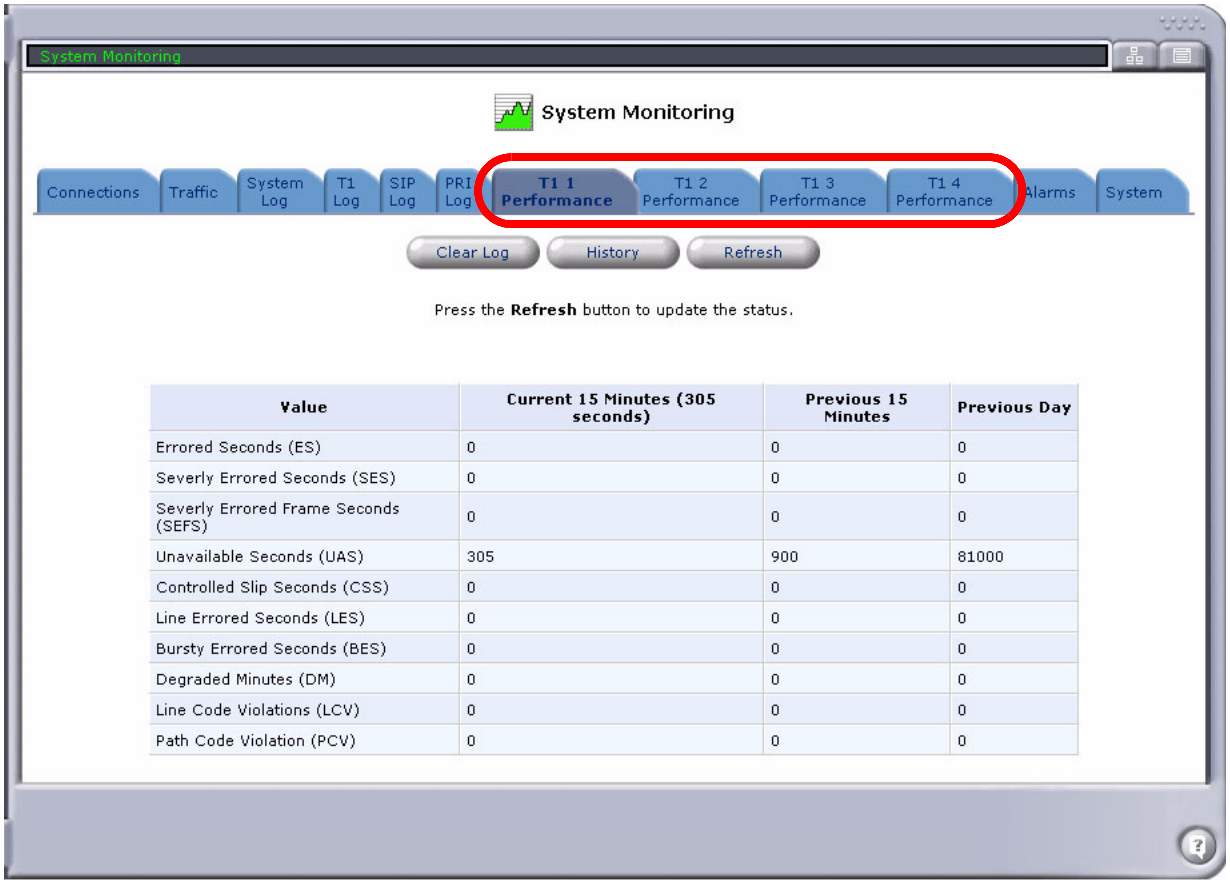
Display Number Of Lines Per Message (0 = full): 1

Press the **Refresh** button to update the status.

Field	Definition
Enable PRI Logging	Use this checkbox to enable (check) or disable (unchecked) PRI logging.
PRI Log Size	Configure the PRI log size. Range is 1 - 50KB, with a default of 50KB.
Buffer Fill Method	Define the method of loading the buffer. **Circular Buffer** - the buffer will store a continuous stream of data by starting again at the beginning of the buffer after reaching the end. Default. **Fill Until Full** - the buffer will fill until it is full. The user will have to clear the log manually.
Display Number of Lines Per Message	Defines the number of lines per message. 0 = full . Default is 1.

T1 Performance (Adit 3000 Only)

The **T1 1** through **T1 4 Performance** tabs display the performance statistics for each of the Adit 3000’s T1s.

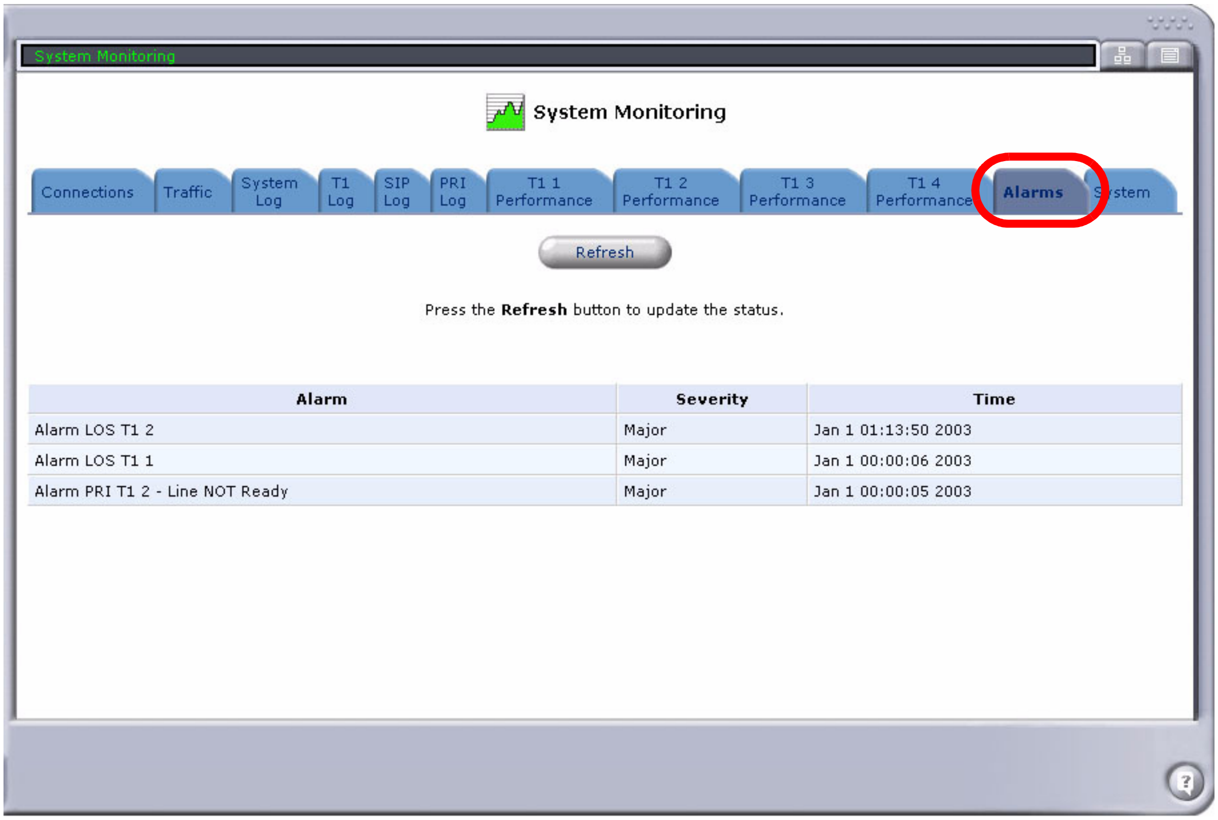


Press the **Refresh** button to update the status.

Value	Current 15 Minutes (305 seconds)	Previous 15 Minutes	Previous Day
Errored Seconds (ES)	0	0	0
Severly Errored Seconds (SES)	0	0	0
Severly Errored Frame Seconds (SEFS)	0	0	0
Unavailable Seconds (UAS)	305	900	81000
Controlled Slip Seconds (CSS)	0	0	0
Line Errored Seconds (LES)	0	0	0
Bursty Errored Seconds (BES)	0	0	0
Degraded Minutes (DM)	0	0	0
Line Code Violations (LCV)	0	0	0
Path Code Violation (PCV)	0	0	0

Alarms

The **Alarms** tab displays the system alarms, their severity, and the time at which each event occured.

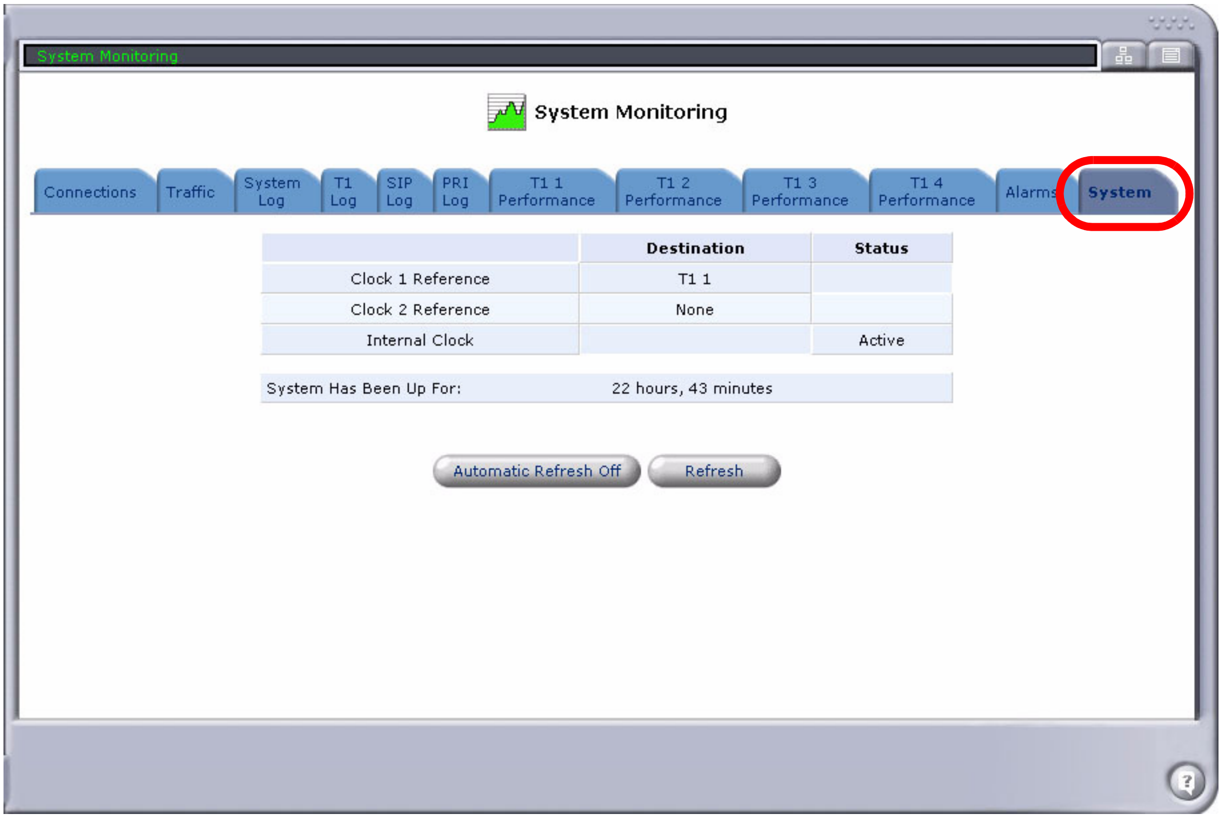


Press the **Refresh** button to update the status.

Alarm	Severity	Time
Alarm LOS T1 2	Major	Jan 1 01:13:50 2003
Alarm LOS T1 1	Major	Jan 1 00:00:06 2003
Alarm PRI T1 2 - Line NOT Ready	Major	Jan 1 00:00:05 2003

System

The **System** tab displays the amount of time that has passed since the system was last started or reset.



	Destination	Status
Clock 1 Reference	T1 1	
Clock 2 Reference	None	
Internal Clock		Active

System Has Been Up For: 22 hours, 43 minutes

CHAPTER 6

Voice Over IP

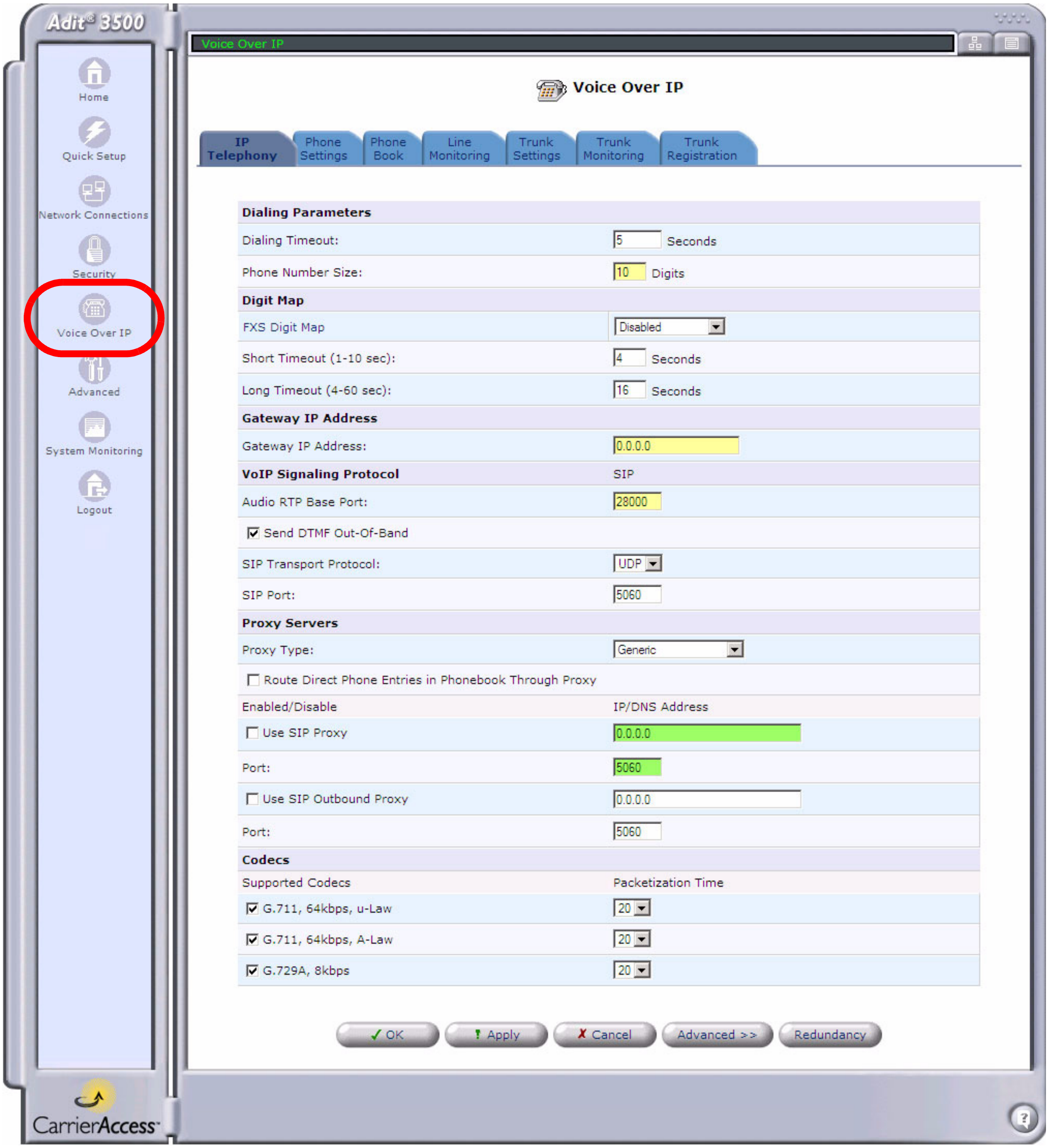
NOTE: This feature is not available on the Adit 3200.

In this Chapter

Overview

The VoIP feature allows you to connect multiple phones over a single broadband connection, providing the benefits and quality of digital voice. The Adit enables you to place and receive calls over the Internet using a standard telephone set connected to the Adit.

WARNING! **ANY CHANGES TO THE VOIP SETTINGS WILL RESTART THE VOIP TASK AND WILL CAUSE ANY ACTIVE CALLS TO BE DROPPED.**

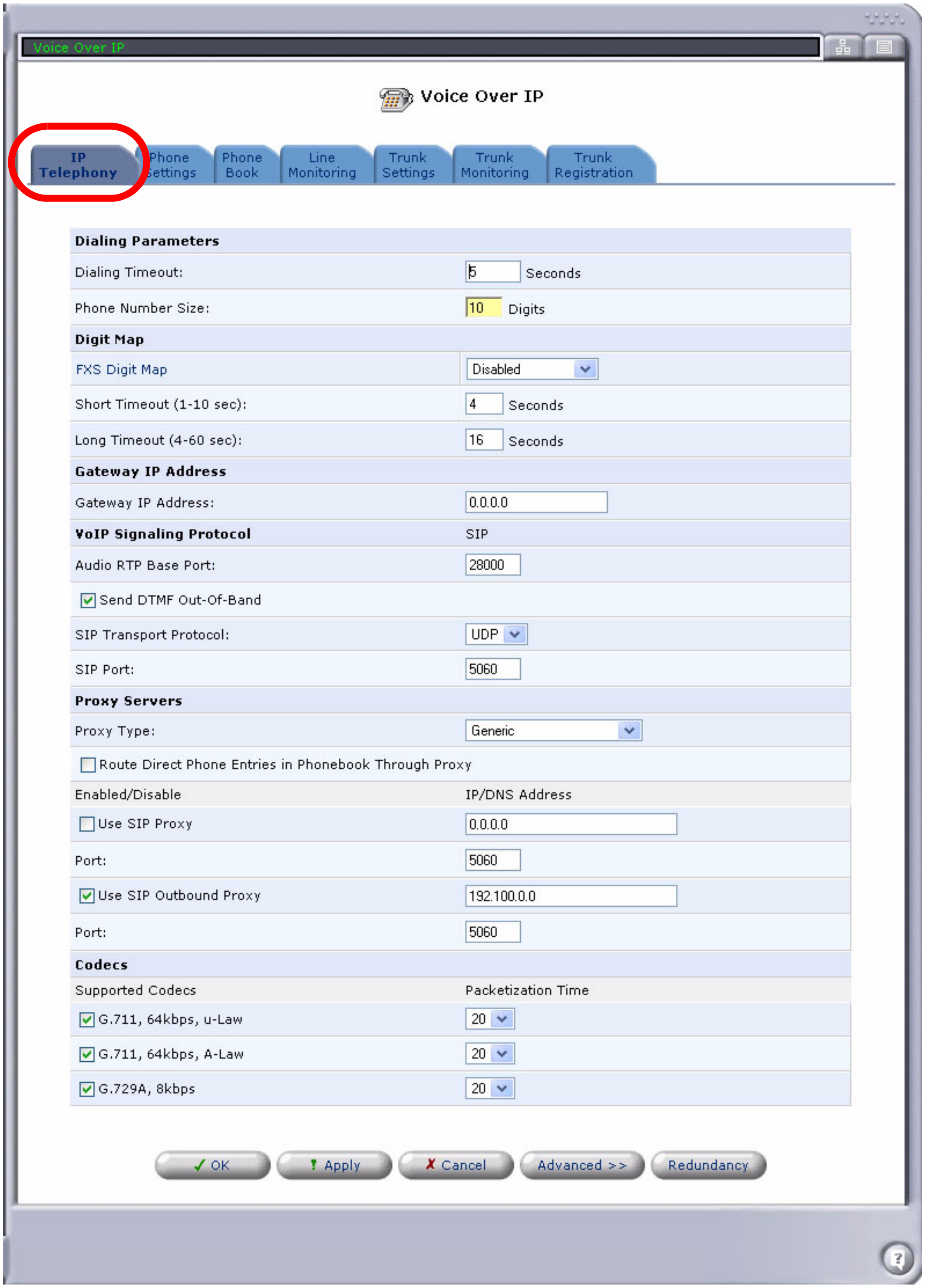


Voice Over IP

Dialing Parameters	
Dialing Timeout:	5 Seconds
Phone Number Size:	10 Digits
Digit Map	
FXS Digit Map	Disabled
Short Timeout (1-10 sec):	4 Seconds
Long Timeout (4-60 sec):	16 Seconds
Gateway IP Address	
Gateway IP Address:	0.0.0.0
VoIP Signaling Protocol	SIP
Audio RTP Base Port:	28000
☑ Send DTMF Out-Of-Band	
SIP Transport Protocol:	UDP
SIP Port:	5060
Proxy Servers	
Proxy Type:	Generic
□ Route Direct Phone Entries in Phonebook Through Proxy	
Enabled/Disable	IP/DNS Address
□ Use SIP Proxy	0.0.0.0
Port:	5060
□ Use SIP Outbound Proxy	0.0.0.0
Port:	5060
Codecs	
Supported Codecs	Packetization Time
☑ G.711, 64kbps, u-Law	20
☑ G.711, 64kbps, A-Law	20
☑ G.729A, 8kbps	20

IP Telephony

Use the **IP Telephony** tab to configure VoIP dialing parameters, signaling protocols, and codecs.



Dialing Parameters	
Dialing Timeout:	5 Seconds
Phone Number Size:	10 Digits
Digit Map	
FXS Digit Map	Disabled
Short Timeout (1-10 sec):	4 Seconds
Long Timeout (4-60 sec):	16 Seconds
Gateway IP Address	
Gateway IP Address:	0.0.0.0
VoIP Signaling Protocol	SIP
Audio RTP Base Port:	28000
☑ Send DTMF Out-Of-Band	
SIP Transport Protocol:	UDP
SIP Port:	5060
Proxy Servers	
Proxy Type:	Generic
□ Route Direct Phone Entries in Phonebook Through Proxy	
Enabled/Disable	IP/DNS Address
□ Use SIP Proxy	0.0.0.0
Port:	5060
☑ Use SIP Outbound Proxy	192.100.0.0
Port:	5060
Codecs	
Supported Codecs	Packetization Time
☑ G.711, 64kbps, u-Law	20
☑ G.711, 64kbps, A-Law	20
☑ G.729A, 8kbps	20

Field	Definition
Dialing Parameters	
Dialing Timeout	Determines how long the system will wait for the next dialed digit before stopping digit-collection. If a digit has been dialed and the number of seconds entered in this field expire, that will be the last digit in the dialed number. Default is 5 seconds.
Phone Number Size	Defines the maximum number of digits in a phone number, range is 3-24. If a number greater than that defined is dialed, the additional digits will be ignored by the system. Default is 10.
Digit Map	
FXS Digit Map	**Disabled** - Use the phone book, maximum digits, or dialing timeout to determine end of dialing. Default. **Default Digit Map** - Pass dialed number as a complete number for routing to the phone book, or to the proxy if there are no phone book entries. **Custom Digit Map** - Process as for the default digit map. See *Configuring the Digit Map on page 6-6*.
Short Timeout	Digit Map Timeout. Short Timeout is used to handle digit map elements containing a **T**. Range is 1-10 seconds.
Long Timeout	Digit Map Timeout. Long Timeout, if it is exceeded, will terminate the dialing sequence. Range is 4-60 seconds.
Gateway IP Address	
Gateway IP Address	The IP address to be used as the source IP for VoIP services when it matches one of the up or running interfaces' IP addresses, otherwise the VoIP source IP address is determined by the previous automatic algorithm.
VoIP Signaling Protocol	**SIP** - Session Initiation Protocol as per RFC 3261.
Audio RTP Base Port	Choice of port to be advertised during the media-negotiation phase of call-setup and used during the call to send and receive RTP. Range is 1024 - 65535. Default is 28000.
Send DTMF Out-of-Band	Selecting this option will send DTMF events as RTP event packets. Otherwise, DTMF events will be sent in-band as part of the RTP packets.
SIP Transport Protocol	Selects the transport layer protocol to be used for carrying SIP payloads. UDP is commonly used and is the default. **TCP** - Transmission Control Protocol. **UDP -** User Datagram Protocol.
SIP Port	Choice of a TCP or UDP port to receive SIP traffic. Enter a numeric value between 1024 and 65535. Default is 5060.

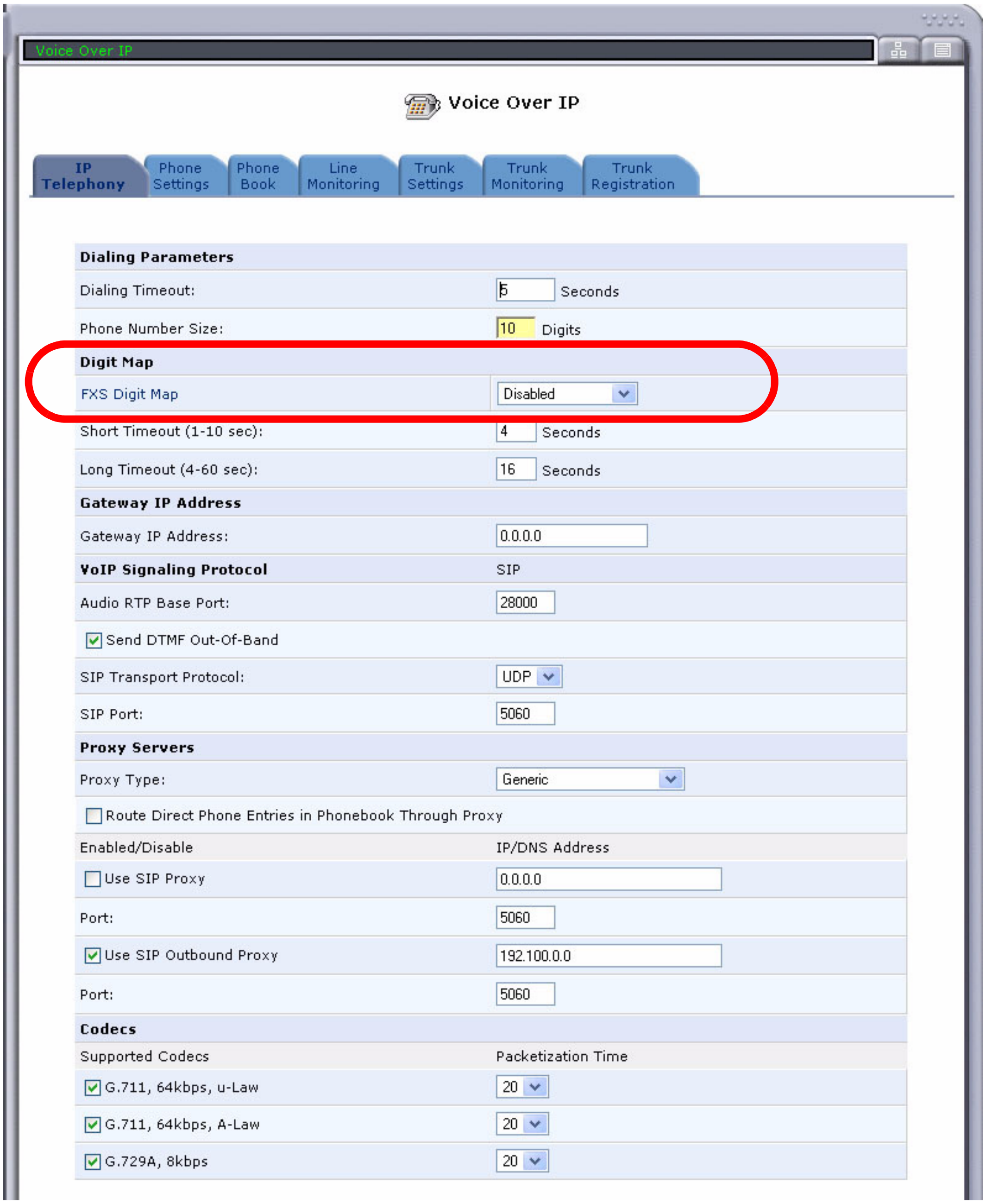
Field	Definition (Continued)
Proxy Servers	
Proxy Type	This drop-down menu allows users to select the proxy type: **Generic** **BroadSoft (Info)** **Sylantro** **Lucent (Info)**
Route Direct Phone Entries in Phone book through Proxy	Select the checkbox to enable.
Enabled/Disable	Enable or disable the features listed below.
Use SIP Proxy	Select to enable, and enter the IP/DNS address of the SIP Proxy.
Port	Enter SIP Proxy port where SIP requests are to be sent. Range is 1024-65535, with a default of 5060.
Use SIP Outbound Proxy	Select to enable, and enter the IP address of the SIP Outbound Proxy. An outbound proxy is one to which all outgoing SIP requests are sent.
Port	Enter SIP Outbound Proxy port. Range is 1024-65535, default of 5060.
Codecs	
Supported Codecs	Allows the user to select which codecs are to be enabled and provides a drop-down menu to select the packetization time (ms): **G.711, 64kbps, u-Law** = 10, 20, 30, 40, 50 or 60 (default is 20) **G.711, 64kbps, A-Law** = 10, 20, 30, 40, 50 or 60 (default is 20) **G.729, 8kbps** = 10, 20, 30, 40, 50, 60, 70 or 80 (default is 20)

Configuring the Digit Map

The Digit Map is used to define phone-specific dialing behavior. A dial plan allows the phone to identify that an entered number is complete and the call should be initiated. If the phone digit map is not defined properly, a (SIP) call may be initiated before the user is done dialing.

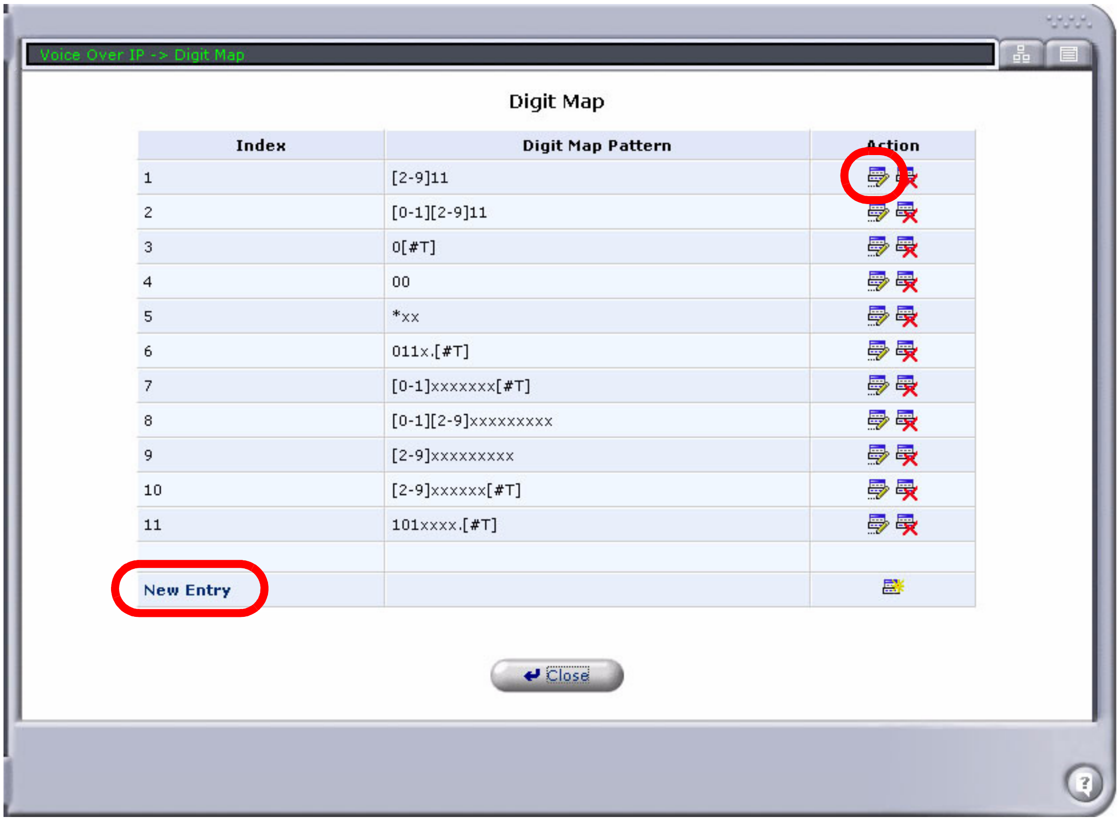
To configure the digit map:

1. Select **Voice over IP**.
2. Select the **IP Telephony** tab.
3. Select **FXS Digit Map**.



Dialing Parameters	
Dialing Timeout:	5 Seconds
Phone Number Size:	10 Digits
Digit Map	
FXS Digit Map	Disabled
Short Timeout (1-10 sec):	4 Seconds
Long Timeout (4-60 sec):	16 Seconds
Gateway IP Address	
Gateway IP Address:	0.0.0.0
VoIP Signaling Protocol	SIP
Audio RTP Base Port:	28000
☑ Send DTMF Out-Of-Band	
SIP Transport Protocol:	UDP
SIP Port:	5060
Proxy Servers	
Proxy Type:	Generic
☐ Route Direct Phone Entries in Phonebook Through Proxy	
Enabled/Disable	IP/DNS Address
☐ Use SIP Proxy	0.0.0.0
Port:	5060
☑ Use SIP Outbound Proxy	192.100.0.0
Port:	5060
Codecs	
Supported Codecs	Packetization Time
☑ G.711, 64kbps, u-Law	20
☑ G.711, 64kbps, A-Law	20
☑ G.729A, 8kbps	20

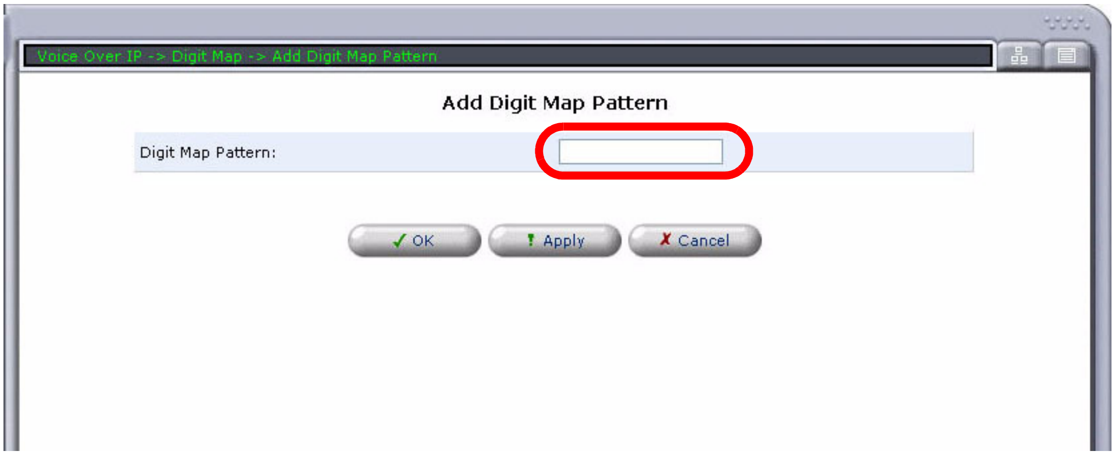
4. Select **New Entry** to create a new Digit Map pattern, or select the Edit icon to modify an existing one.



Digit Map

Index	Digit Map Pattern	Action
1	[2-9]11	
2	[0-1][2-9]11	
3	0[#T]	
4	00	
5	*xx	
6	011x.[#T]	
7	[0-1]xxxxxxx[#T]	
8	[0-1][2-9]xxxxxxxxx	
9	[2-9]xxxxxxxxx	
10	[2-9]xxxxxx[#T]	
11	101xxxx.[#T]	
New Entry		

5. Enter the new digit map pattern and select **OK**.



Add Digit Map Pattern

Digit Map Pattern:

Digit Map Pattern

A Digit Map Pattern consists of a sequence of one or more of the following character or string elements:

Character/String	Definition
digit	**1 - 9**
special keypad character	*****, **#**, **a**, **b**, **c** or **d**
wildcard digit	**x** or **?** (which represents any numerical digit)
super wildcard	**.** or **$** (which indicates 0 or more digits of the previous type)
short timeout character	**T**
range element	[**<rrr>**] where **<rrr>** may consist of one or more elements of the following type: **digit range d-d** - where the first **d** is a digit, and the second **d** is a higher digit **character c** - where **c** is any digit, special keypad character or **T**.

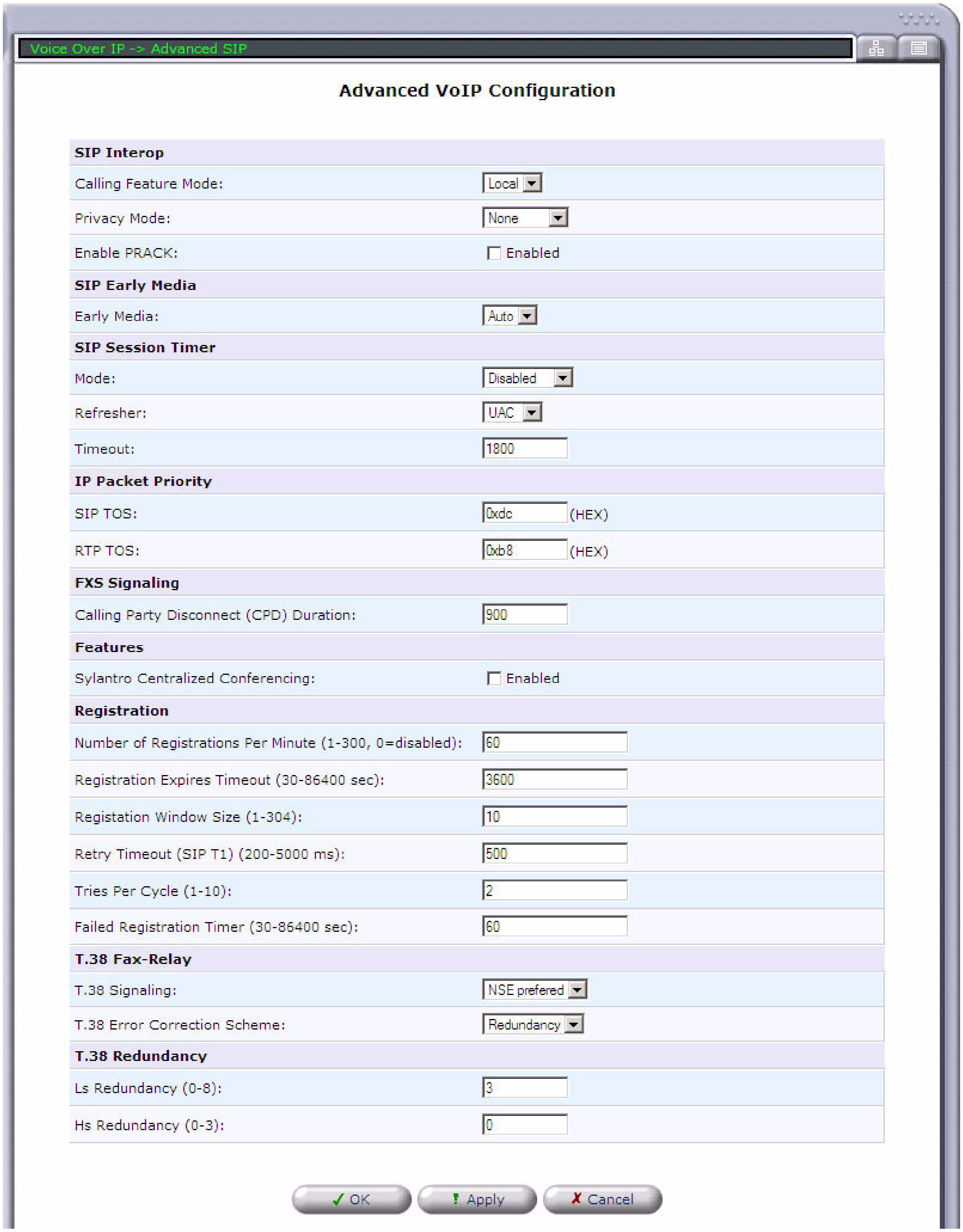
The maximum number of characters in the string is 500. Up to 30 patterns can be entered.

Example: [2-9]xxxxx[#T]

This example represents a 7-digit number, beginning with a digit between 2 and 9, and ending with either a short timeout or by the user pressing the # key character. **Note:** The # is not considered part of the number if it is at the end of the dial-string.

Advanced (Button)

The **Advanced** button at the bottom of the **IP Telephony** window opens a window for configuring the Advanced VoIP (SIP) settings.



Voice Over IP -> Advanced SIP

Advanced VoIP Configuration

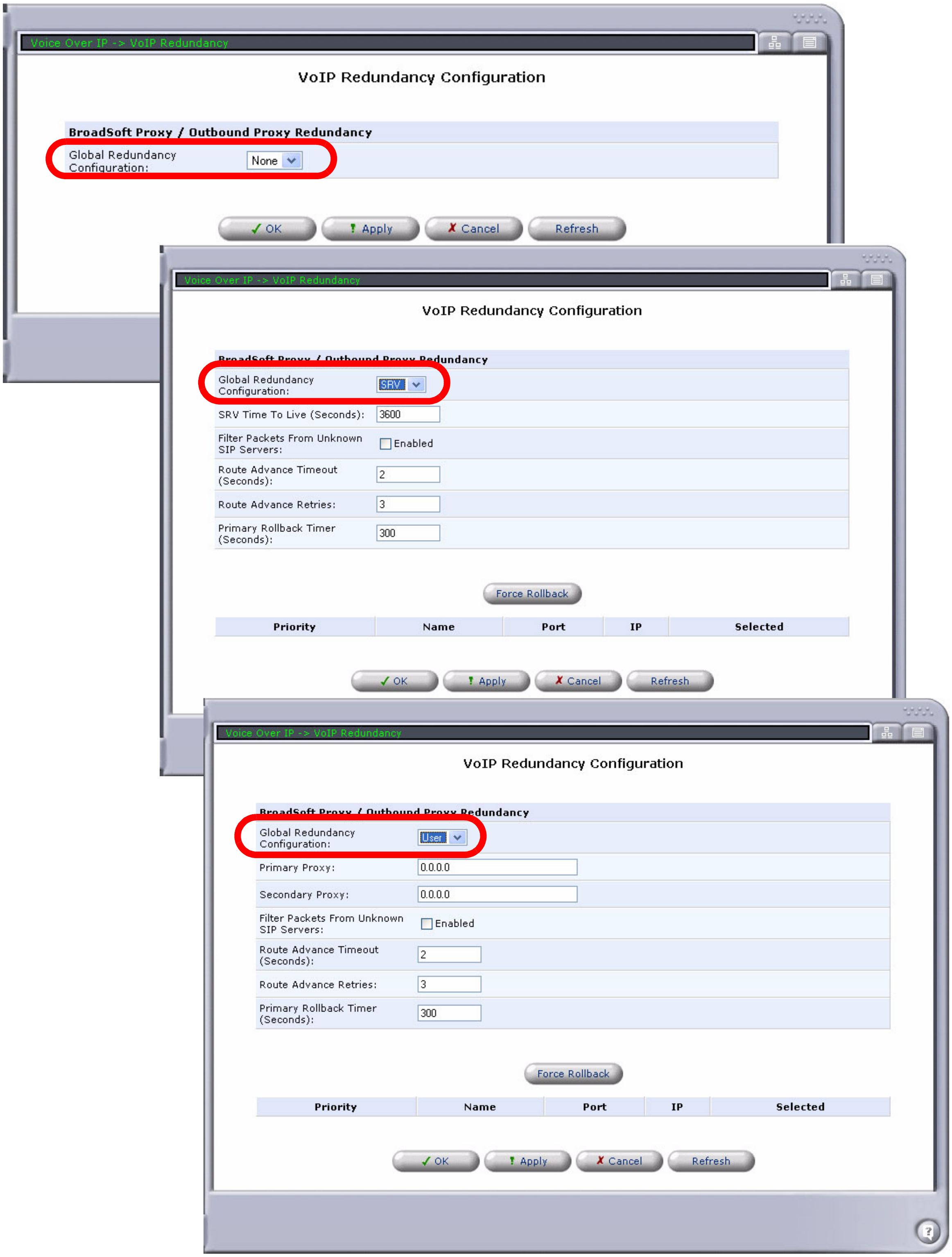
SIP Interop	
Calling Feature Mode:	Local
Privacy Mode:	None
Enable PRACK:	□ Enabled
SIP Early Media	
Early Media:	Auto
SIP Session Timer	
Mode:	Disabled
Refresher:	UAC
Timeout:	1800
IP Packet Priority	
SIP TOS:	0xdc (HEX)
RTP TOS:	0xb8 (HEX)
FXS Signaling	
Calling Party Disconnect (CPD) Duration:	900
Features	
Sylantro Centralized Conferencing:	□ Enabled
Registration	
Number of Registrations Per Minute (1-300, 0=disabled):	60
Registration Expires Timeout (30-86400 sec):	3600
Registation Window Size (1-304):	10
Retry Timeout (SIP T1) (200-5000 ms):	500
Tries Per Cycle (1-10):	2
Failed Registration Timer (30-86400 sec):	60
T.38 Fax-Relay	
T.38 Signaling:	NSE prefered
T.38 Error Correction Scheme:	Redundancy
T.38 Redundancy	
Ls Redundancy (0-8):	3
Hs Redundancy (0-3):	0

Field	Definition
SIP Interop	
Calling Feature Mode	Determines where the intelligence for the calling features will lie, offering a choice between server-based (Info) and device-based (local) features. **Info** - This selection is used with BroadSoft 11.1 Info Mode Proxy. **Note:** On a BroadSoft server, the Adit must be configured as “Generic SIP Standard (Proxy Address)”. **Local** - Default.
Privacy Mode	**None** - Disables the Privacy Mode. Default. **RFC-3325** - Enables support for RFC 3325, as supported on the Sylantro Application Server.
Enable PRACK	Allows the user to enable/disable Provisional Acknowledgement (PRACK), as per RFC 3262. Default is Disabled.
SIP Early Media	
Early Media	Early Media is the ability of two SIP user agents to communicate before a SIP call is actually established. Support for early media is important largely for interoperability with the PSTN. This field allows the user to control which 18*n* response is sent by the Adit on calls from SIP-to PRI/CAS. **Auto -** Send 180/183, based on if in-band call progress tones are available. **180 -** Always sent 180, with or without SDP. The 180 Ringing message is a provisional or informational response used to indicate that the INVITE message has been received by the user agent and that alerting is taking place. **183 -** Always sent 183, with or without SDP. The 183 Session Progress response indicates that information about the call state is present in the message body media information. **Note:** Both 180 and 183 messages may contain SDP, which allows an early media session to be established prior to the call being answered.
SIP Session Timer	
Mode	**Disabled** - System shall not initiate Session Timer procedures, nor respond to a Session-Expires request. Default. **Supported** - System will respond to a Session-Expires request from a remote proxy or UAC. **Requested** - System shall initiate Session Timer procedures in outgoing initial INVITEs by including a Session-Expires header.
Refresher	**None** - No refresher parameter shall be sent in an INVITE, and any refresher received from the remote proxy or UAC shall be echoed back. **UAC** - User Agent Client. Default. **UAS** - User Agent Server.
Timeout	Range is 90-7200 seconds, with a default of 1800.
IP Packet Priority - Sets the precedence bits in the TOS byte of the IP header to prioritize packet handling.	
RTP TOS	Range is 0x00 - 0xff. Default 0xb8
SIP TOS	Range is 0x00 - 0xff. Default 0xdc

Field	Definition (Continued)
FXS Signaling	
Calling Party Disconnect (CPD) Duration	Allows the user to configure the disconnect timeout for individual lines. Range is 500 - 3000. Default is 900.
Features	
Sylantro Centralized Conferencing	Enables the “Centralized Three-Way Calling” feature with the Sylantro application server. This provides the means for an FXS telephone user to place an existing SIP call on hold, dial a second SIP call, then connect all 3 parties together.
Registration - Allows SIP URI registration for each number assiged to an FXS or trunk line.	
Number of Registration per Minute	Range 1 - 300. 0 = disabled. Default is 60.
Registration Expires Timeout	Range 30 - 86400 Seconds. Default is 3600 seconds.
Registration Window Size	Range 1 - 304. Default is 10.
Retry Timeout (SIP T1)	Range 200 - 4000 milliseconds. Default is 500.
Tries Per Cycle	Range 1 - 10. Default is 2.
Failed Registration Timer	Range is 300 - 86400 seconds. Default is 60.
T.38 Fax-Relay **Note:** For the Adit 3000, this feature is available only when the Adit is configured with the FXS option. **Note:** For the Adit MSR, T.38 will be supported in a future release.	
T.38 Signaling	**NSE Only** - NSE (Named Service Event) will be the only method tried. **NSE Preferred** - NSE preferred will be the first method tried, with an attempt to the alternate SDP method if it fails. Default. **SDP Only** - SDP (Session Description Protocol) will be the only method tried. **SDP Preferred** - SDP preferred will be the first method tried, with an attempt to the alternate NSE method if it fails
T.38 Error Detection Scheme	**None** - Set error correction to none. **Redundancy** - A T.38 data stream is transmitted with redundant (duplicated) data and checksums (CRCs). This way, if the receiving gateway detects that a packet has been lost or corrupted, it can extract it from the redundant data.
T.38 Redundancy **Note:** For the Adit 3000, this feature is available only when the Adit is configured with the FXS option. **Note:** For the Adit MSR, T.38 will be supported in a future release.	
Ls Redundancy	Range 0 to 8 packets (0 = no redundancy), with a default of 3 packets. Configures the number of duplicate packets to transmit during a low-speed T.38 fax call.
Hs Redundancy	Range 0-3 packets, with a default of 0 packets (no redundancy). Configures the number of duplicate packets to transmit during a high-speed T.38 fax call. **Note:** Setting the HS Redundancy parameter greater than 0 will cause a significant increase in the network bandwidth consumed by the fax call.

Redundancy (Button)

The **Redundancy** button at the bottom of the **IP Telephony** window opens a window for configuring VoIP proxy redundancy. **Note:** This window is modified upon selection of the Global Redundancy Configuration field.



VoIP Redundancy Configuration

BroadSoft Proxy / Outbound Proxy Redundancy

Global Redundancy Configuration:	None

VoIP Redundancy Configuration

BroadSoft Proxy / Outbound Proxy Redundancy

Global Redundancy Configuration:	SRV
SRV Time To Live (Seconds):	3600
Filter Packets From Unknown SIP Servers:	□ Enabled
Route Advance Timeout (Seconds):	2
Route Advance Retries:	3
Primary Rollback Timer (Seconds):	300

Priority	Name	Port	IP	Selected

VoIP Redundancy Configuration

BroadSoft Proxy / Outbound Proxy Redundancy

Global Redundancy Configuration:	User
Primary Proxy:	0.0.0.0
Secondary Proxy:	0.0.0.0
Filter Packets From Unknown SIP Servers:	□ Enabled
Route Advance Timeout (Seconds):	2
Route Advance Retries:	3
Primary Rollback Timer (Seconds):	300

Priority	Name	Port	IP	Selected

When the primary proxy is not reachable or returns an error, the system initiates a rollover (the next server in the list is used, until a working server replies).

When the last server in the list fails, the rollover is considered a rollback. The route advance timeout will not take effect for 30 seconds and retransmission timers will take precedence. After 30 seconds, the primary proxy (first in the list) will be treated as active again.

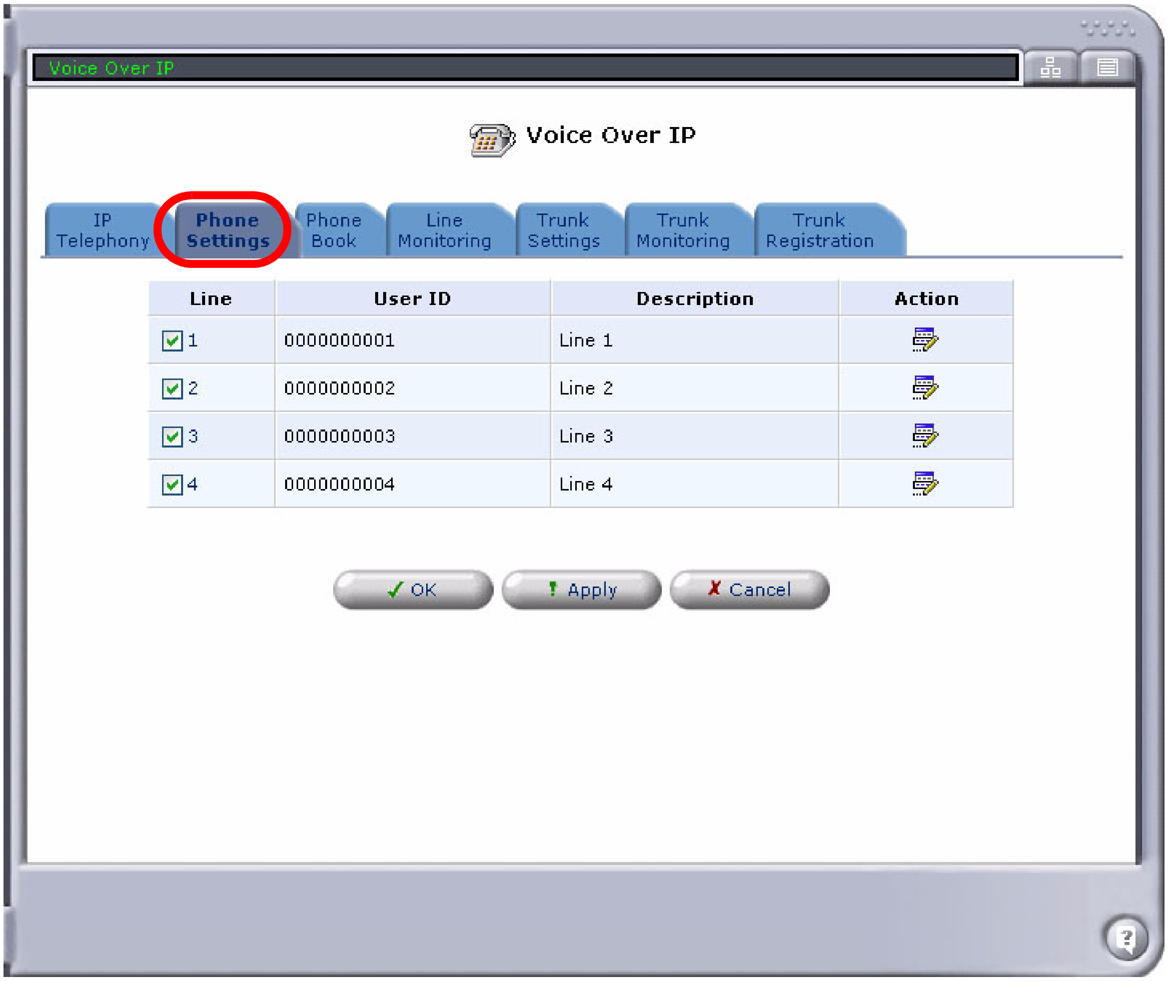
Field	Definition
BroadSoft Proxy/Outbound Proxy Redundancy	
Global Redundancy Configuration	**None** - Redundancy feature is disabled. Default. **SRV** - An SRV lookup will be performed using the main proxy. The hosts/IPs found are used to form the proxy redundancy list. **User** - The SIP messages will be sent to the primary proxy. If there is a failure, it will be sent to the secondary proxy.
SRV Time to Live (seconds)	A set interval of time between flushing the SRV cache. Range is 0 - 3600 seconds, with a default of 3600 (1 hr.). 0 = Cancel this feature. **Note:** This field appears only when **SRV** is selected in the Global Redundancy Configuration field.
Primary Proxy	Enter Primary Outbound Proxy address. **Note:** This field appears only when **User** is selected in the Global Redundancy Configuration field.
Secondary Proxy	Enter Secondary Outbound Proxy address. **Note:** This field appears only when **User** is selected in the Global Redundancy Configuration field.
Filter Packets from Unknown SIP Servers	Select checkbox to enable filtering.
Router Advance Timeout (seconds)	A set interval of time before moving onto the next proxy when the first is not reachable. Range is 0 - 10 seconds, with a default of 2.
Route Advance Retries	A set number of retries before a proxy is considered unreachable and moving onto the next. Range is 0 - 10, with a default of 3.
Primary Rollback Timer (seconds)	A set interval of time between the time the primary proxy fails and when a rollback is performed back to the primary proxy. Range is 60 to 3600 seconds or 0 (disabled). Default is 300 seconds (5 minutes).
Force Rollback (button) - When this button is selected, the primary proxy will be considered active and all new subsequent transactions will be sent to the primary. Normal rollover will apply after this.	
Priority	Displayed by priority.
Name	Host name.
Port	Proxy port.
IP	Host IP address.
Selected	Indicates current proxy.

Phone Settings

Use the **Phone Settings** tab to configure each line for VoIP.

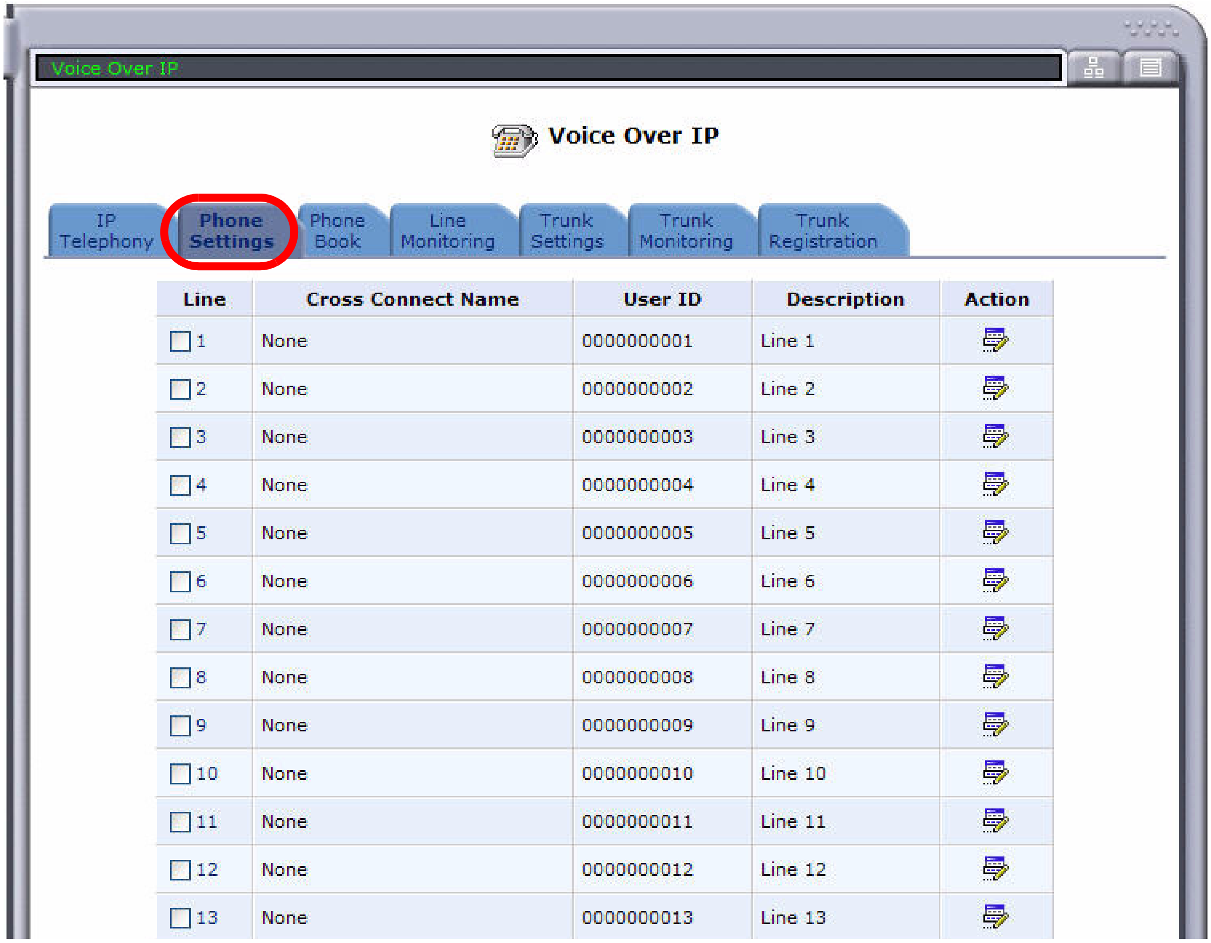
NOTE: When connecting analog lines to the PBX, impedance settings can be used to match impedance between the analog interfaces. Consult the PBX, Key System, or connecting equipment manual.

Adit 3500



Line	User ID	Description	Action
☑ 1	0000000001	Line 1	✎
☑ 2	0000000002	Line 2	✎
☑ 3	0000000003	Line 3	✎
☑ 4	0000000004	Line 4	✎

Adit MSR

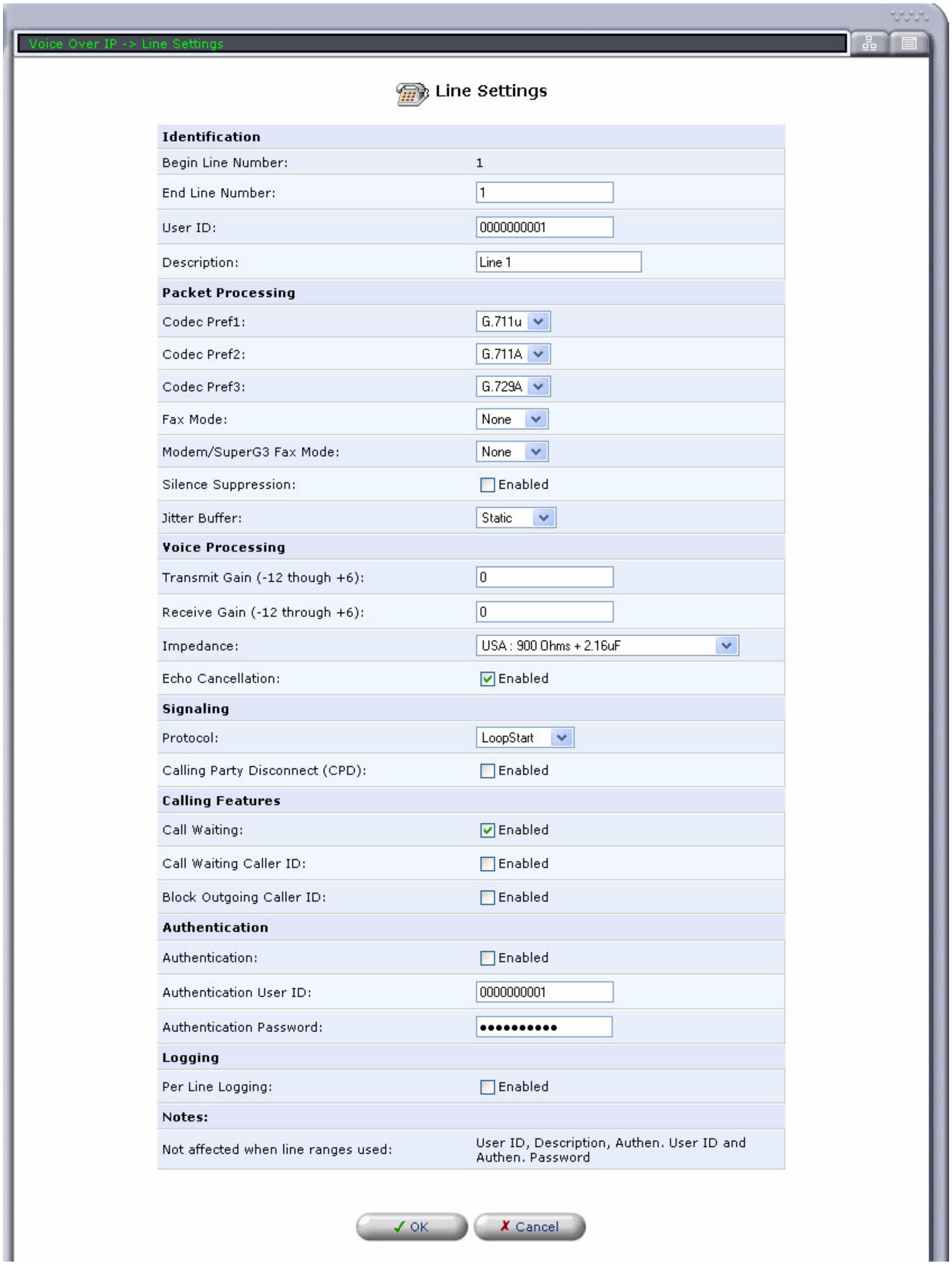


Line	Cross Connect Name	User ID	Description	Action
□ 1	None	0000000001	Line 1	✎
□ 2	None	0000000002	Line 2	✎
□ 3	None	0000000003	Line 3	✎
□ 4	None	0000000004	Line 4	✎
□ 5	None	0000000005	Line 5	✎
□ 6	None	0000000006	Line 6	✎
□ 7	None	0000000007	Line 7	✎
□ 8	None	0000000008	Line 8	✎
□ 9	None	0000000009	Line 9	✎
□ 10	None	0000000010	Line 10	✎
□ 11	None	0000000011	Line 11	✎
□ 12	None	0000000012	Line 12	✎
□ 13	None	0000000013	Line 13	✎

NOTE: To display all available lines on the MSR, select **Display All Lines**. To display only cross-connected lines, select **Display Cross Connect Lines**.

Configuring Phone Settings

1. Select the **Phone Settings** tab on the **Voice over IP** window.
2. Select the **Action** icon for the line to configure.
3. Set the **Line Settings** as desired. See the following table for field definitions.



Voice Over IP -> Line Settings

Line Settings

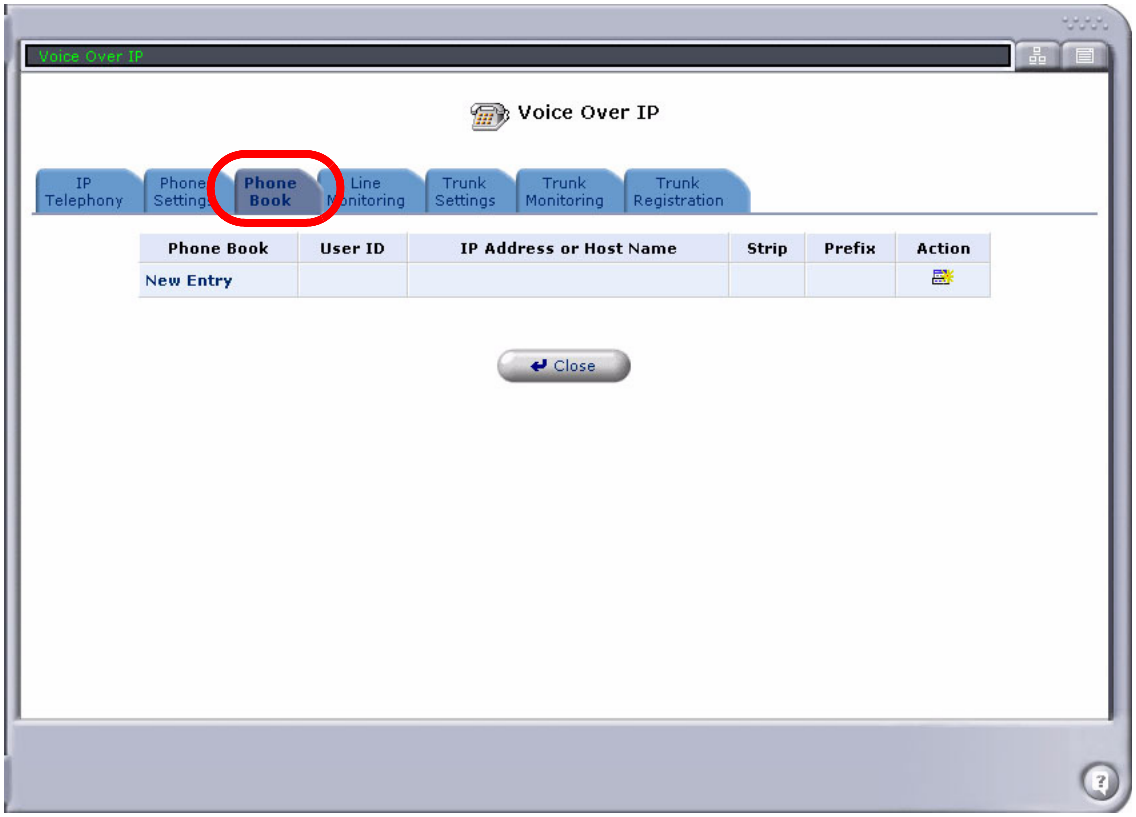
Identification	
Begin Line Number:	1
End Line Number:	1
User ID:	0000000001
Description:	Line 1
Packet Processing	
Codec Pref1:	G.711u
Codec Pref2:	G.711A
Codec Pref3:	G.729A
Fax Mode:	None
Modem/SuperG3 Fax Mode:	None
Silence Suppression:	□ Enabled
Jitter Buffer:	Static
Voice Processing	
Transmit Gain (-12 though +6):	0
Receive Gain (-12 through +6):	0
Impedance:	USA : 900 Ohms + 2.16uF
Echo Cancellation:	☑ Enabled
Signaling	
Protocol:	LoopStart
Calling Party Disconnect (CPD):	□ Enabled
Calling Features	
Call Waiting:	☑ Enabled
Call Waiting Caller ID:	□ Enabled
Block Outgoing Caller ID:	□ Enabled
Authentication	
Authentication:	□ Enabled
Authentication User ID:	0000000001
Authentication Password:	••••••••••
Logging	
Per Line Logging:	□ Enabled
Notes:	
Not affected when line ranges used:	User ID, Description, Authen. User ID and Authen. Password

Field	Definition
Identification	
Begin Line Number	Displays the line number that was selected to edit.
End Line Number	Specifying a line number here allows a user to define a range to apply the settings to. Settings will be applied to all the lines between "begin line number" and "end line number".
User ID	Display/Edit the current User ID. **Note:** A maximum of 20 characters is allowed.
Cross Connect Name	This field appears for the MSR only.
Description	Display/Edit the line description. Use the display name for Caller ID.
Packet Processing	
Codec Pref1	Codec preferences are used to establish the codec list offered during media negotiation. Pref1 is the first codec, followed by pref2 and pref3. Select the first codec preference.
Codec Pref2	Select the second codec preference.
Codec Pref3	Select the third codec preference.
Fax Mode	**None** - A Fax call would be treated as a normal voice call. Default. **Bypass** - Causes the line to transmit in G.711 mode, with silence suppression disabled, on detection of Fax tone.
Modem/SuperG3 Fax Mode	**None -** A Modem call would be treated as a normal voice call. Default. **Bypass -** Causes the line to transmit in G.711 mode, with echo cancellation and silence suppression disabled, on detection of Modem tone.
Silence Suppression	Select to enable Silence suppression on the line.
Jitter Buffer	Set Jitter Buffer from the pulldown menu. **Static -** Maintain a static average delay, through the jitter buffer. Default. **Dynamic** - Specify dynamic delay adjustment to minimize delay through the jitter buffer.
Voice Processing	
Transmit Gain	Set transmit gain. Range -12 to +6. Transmit direction is from the Adit towards FXS.
Receive Gain	Set receive gain. Range -12 to +6. Transmit direction is from the FXS towards the Adit.
Impedance	Set the impedance from the pulldown menu. **Note:** Not supported by the MSR. (Impedance is handled by the Adit 600 controller or card.)
Echo Cancellation	Select to enable Echo Cancellation on the lines.

Field	Definition (Continued)
Signaling	
Protocol	Select the analog signaling mechanism: **Loop Start -** Sets the line to Loop Start signaling. **Ground Start -** Sets the line to Ground Start signaling. **Note:** For the MSR, this field is not selectable. The setting is based on the cross-connect type info.
Calling Party Disconnect (CPD)	Enables/disables Calling Party Disconnect capability for this line. If enabled, causes a timed Open Switching Interval (OSI) to be applied to the FXS loop when the remote (SIP) party disconnects.
Calling Features	
Call Waiting	Enables/disables the Call Waiting capability for this line.
Call Waiting Caller ID	Enables/disables the Call Waiting Caller ID for this line.
Block Outgoing Caller ID	Enables/disables blocking of Caller ID on SIP calls made from this line.
Authentication	
Authentication	Select to enable Authentication on the line.
Authentication User ID	The User ID to be used when responding to authentication requests. Default is the User ID of the line.
Authentication Password	The password to be used when responding to authentication requests.
Logging	
Per Line Logging	Use the checkbox to enable per line logging. Default is unchecked.
Notes	Displays information regarding the current tab.

Phone Book

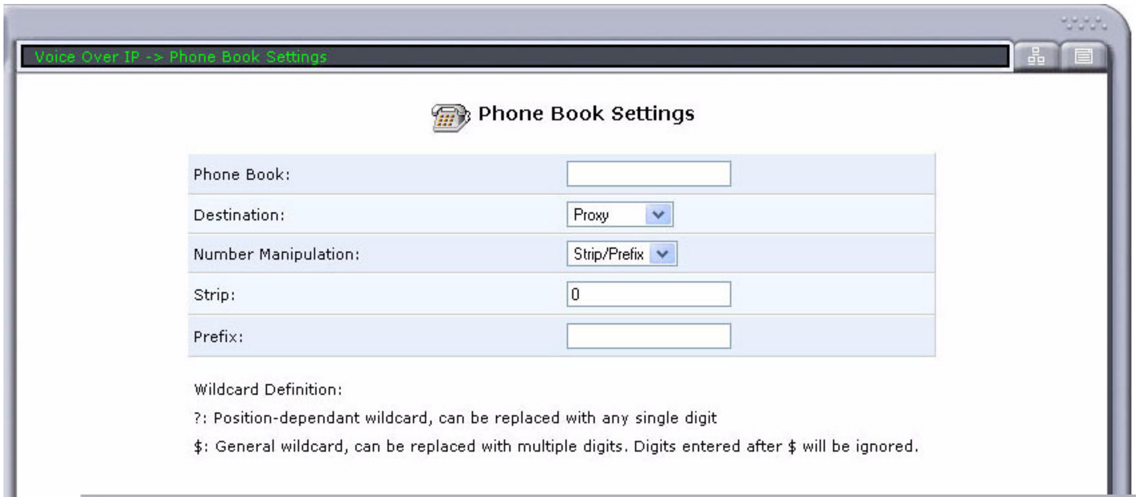
Use the **Phone Book** tab to define the Speed Dial settings. You can define a maximum of 50 entries.



Phone Book	User ID	IP Address or Host Name	Strip	Prefix	Action
New Entry					

Configuring Phone Book Settings

1. Select **Voice over IP/Phone Book** tab.
2. Select **New Entry**. **Note:** This window modifies as the **Destination** field is changed. See the following table for field definitions.



Voice Over IP -> Phone Book Settings

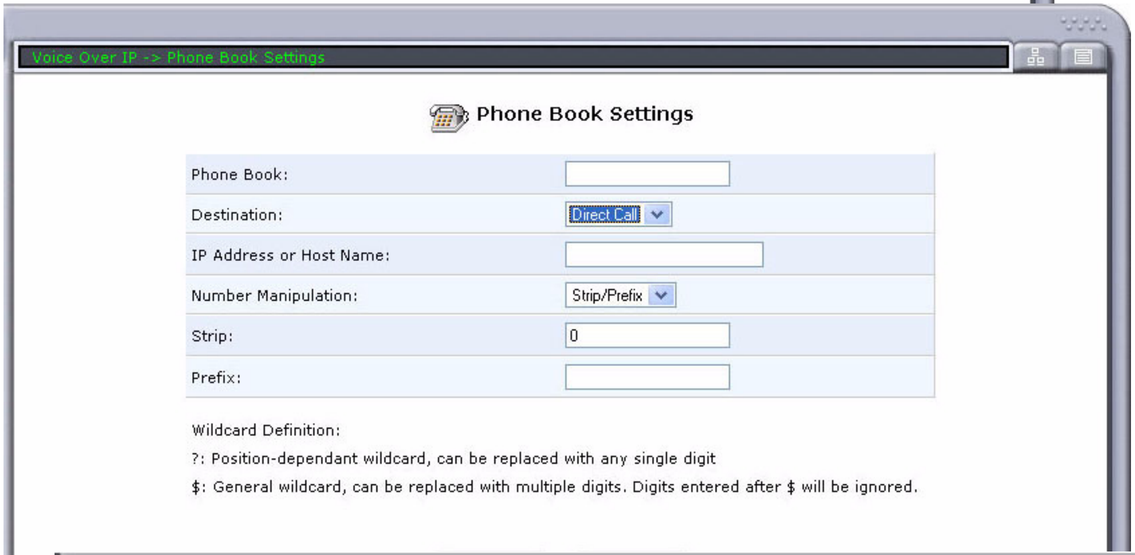
Phone Book Settings

Phone Book:	
Destination:	Proxy
Number Manipulation:	Strip/Prefix
Strip:	0
Prefix:	

Wildcard Definition:

?: Position-dependant wildcard, can be replaced with any single digit

$: General wildcard, can be replaced with multiple digits. Digits entered after $ will be ignored.



Voice Over IP -> Phone Book Settings

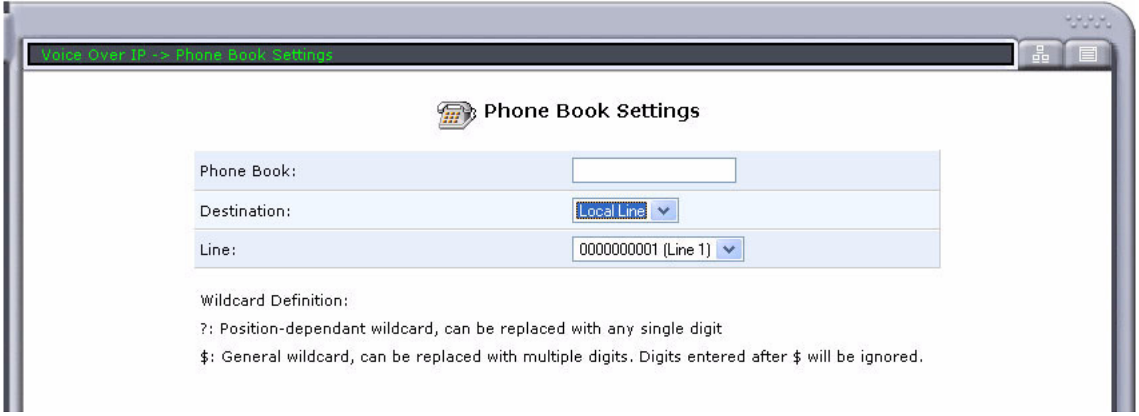
Phone Book Settings

Phone Book:	
Destination:	Direct Call
IP Address or Host Name:	
Number Manipulation:	Strip/Prefix
Strip:	0
Prefix:	

Wildcard Definition:

?: Position-dependant wildcard, can be replaced with any single digit

$: General wildcard, can be replaced with multiple digits. Digits entered after $ will be ignored.



Voice Over IP -> Phone Book Settings

Phone Book Settings

Phone Book:	
Destination:	Local Line
Line:	0000000001 (Line 1)

Wildcard Definition:

?: Position-dependant wildcard, can be replaced with any single digit

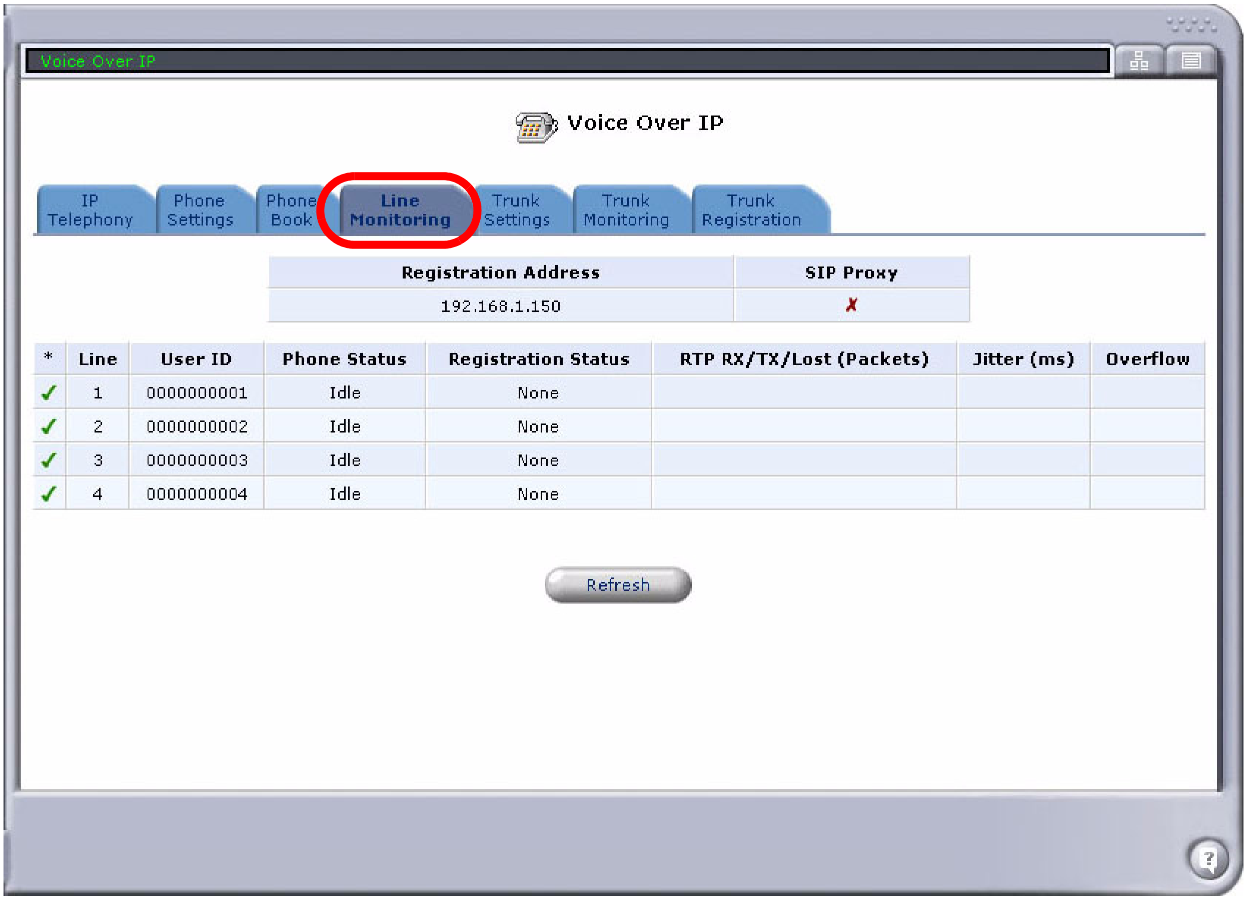
$: General wildcard, can be replaced with multiple digits. Digits entered after $ will be ignored.

Field	Definition
Phone Book	Enter the Speed Dial number. Range is 3-10 digits. This is the number that needs to be dialed to get to this entry. Digits allowed 0-9, #, *, ?, $.
Destination	Phone destination is used to identify the destination of the incoming phone call. The options below are selected from the pulldown menu.
Proxy	Will send INVITE to defined SIP Proxy from IP Telephony tab. Call-setup information is routed through the proxy. **Number Manipulation** **Strip/Prefix -** Modifies the window to display Strip and Prefix fields. **Strip** - The number of digits to be stripped off from the left-most digits in the phone number. Possible usages include stripping off the area code, or the 3-digit office prefix. Range is 0 - 7, with a default of 0. **Prefix** - The digits or name to be added to the phone number after the stripping process has been applied. This field is empty by default. **User ID** - Enter a User ID with a maximum of 20 characters.
Local Line	Will send an INVITE to a local line. Call-setup information does not leave the system. **Line** - Select the line from the pulldown menu.
Direct Call	Will send an INVITE to the User ID and IP address supplied in the Speed Dial configuration for this entry. Call-setup information is sent directly to the IP configured, without using a proxy. **IP Address or Host Name** - Enter an IP Address or Host Name destination. **Number Manipulation** **Strip/Prefix -** Modifies the window to display Strip and Prefix fields. **Strip** - The number of digits to be stripped off from the left-most digits in the phone number. Possible usages include stripping off the area code, or the 3-digit office prefix. Range is 0 - 7, with a default of 0. **Prefix** - The digits or name to be added to the phone number after the stripping process has been applied. This field is empty by default. **User ID** - Enter a User ID with a maximum of 20 characters.

Line Monitoring

The **Line Monitoring** tab displays current information for each line.

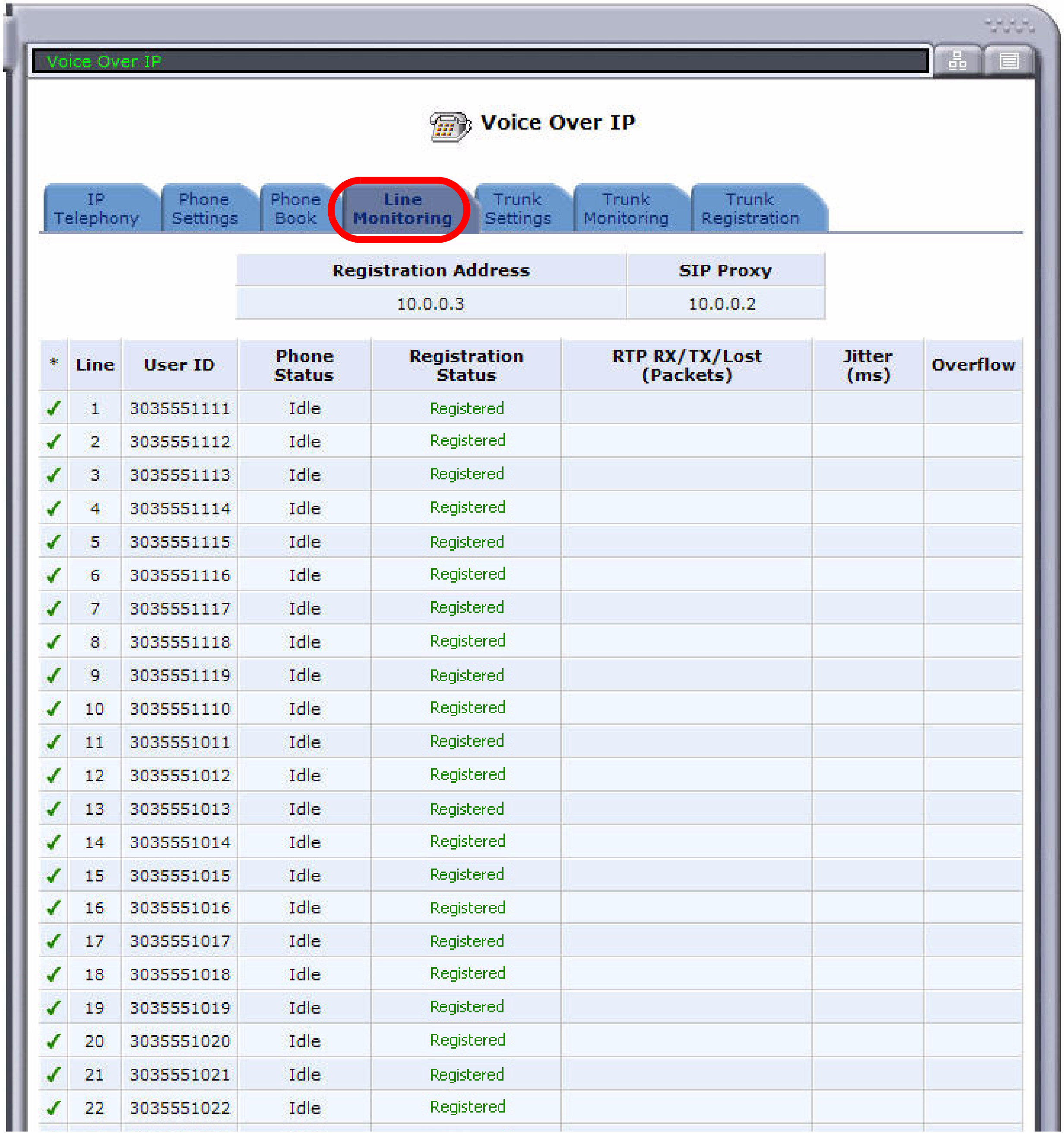
Adit 3500



Registration Address	SIP Proxy
192.168.1.150	✗

*	Line	User ID	Phone Status	Registration Status	RTP RX/TX/Lost (Packets)	Jitter (ms)	Overflow
✓	1	0000000001	Idle	None			
✓	2	0000000002	Idle	None			
✓	3	0000000003	Idle	None			
✓	4	0000000004	Idle	None			

Adit MSR



Registration Address	SIP Proxy
10.0.0.3	10.0.0.2

*	Line	User ID	Phone Status	Registration Status	RTP RX/TX/Lost (Packets)	Jitter (ms)	Overflow
✓	1	3035551111	Idle	Registered			
✓	2	3035551112	Idle	Registered			
✓	3	3035551113	Idle	Registered			
✓	4	3035551114	Idle	Registered			
✓	5	3035551115	Idle	Registered			
✓	6	3035551116	Idle	Registered			
✓	7	3035551117	Idle	Registered			
✓	8	3035551118	Idle	Registered			
✓	9	3035551119	Idle	Registered			
✓	10	3035551110	Idle	Registered			
✓	11	3035551011	Idle	Registered			
✓	12	3035551012	Idle	Registered			
✓	13	3035551013	Idle	Registered			
✓	14	3035551014	Idle	Registered			
✓	15	3035551015	Idle	Registered			
✓	16	3035551016	Idle	Registered			
✓	17	3035551017	Idle	Registered			
✓	18	3035551018	Idle	Registered			
✓	19	3035551019	Idle	Registered			
✓	20	3035551020	Idle	Registered			
✓	21	3035551021	Idle	Registered			
✓	22	3035551022	Idle	Registered			

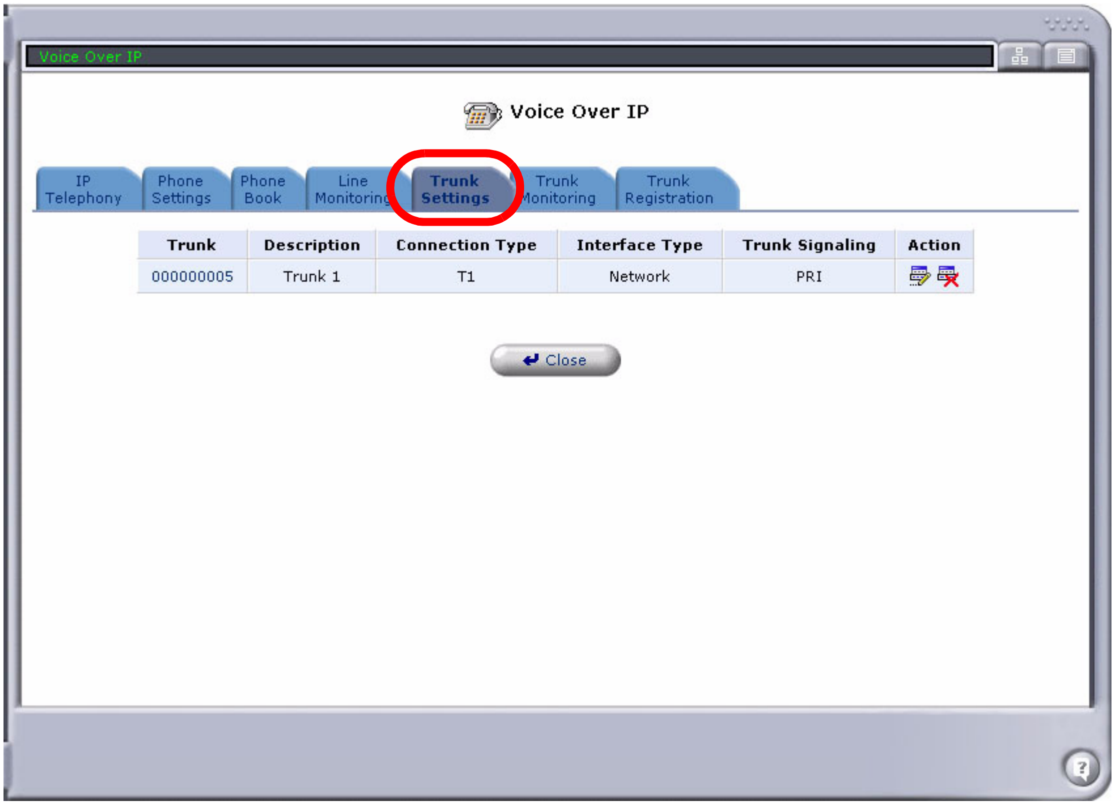
The following table defines the fields displayed in the **Line Monitoring** window:

Field	Definition
Registration Address	Adit WAN IP address. Blank if a proxy has not been selected.
SIP Proxy	Indicates if SIP proxy is selected or not.
Line	Specific FXS line.
User ID	Displays the User ID.
Phone Status	Displays the Phone status - Idle, dialing in progress, ringing, call in progress, etc.
Registration Status	Displays registration status - Registered or failed.
RTP RX/TX/Lost (Packets)	Packets received/transmitted/dropped.
Jitter (ms)	Milliseconds of Jitter incurred on the call.
Overflow	There are too many packets to buffer.

Trunk Settings

NOTE: The **Trunk Settings** tab is only available on the Adit 3500 and Adit MSR.

Use the **Trunk Settings** tab to configure settings for the trunk.

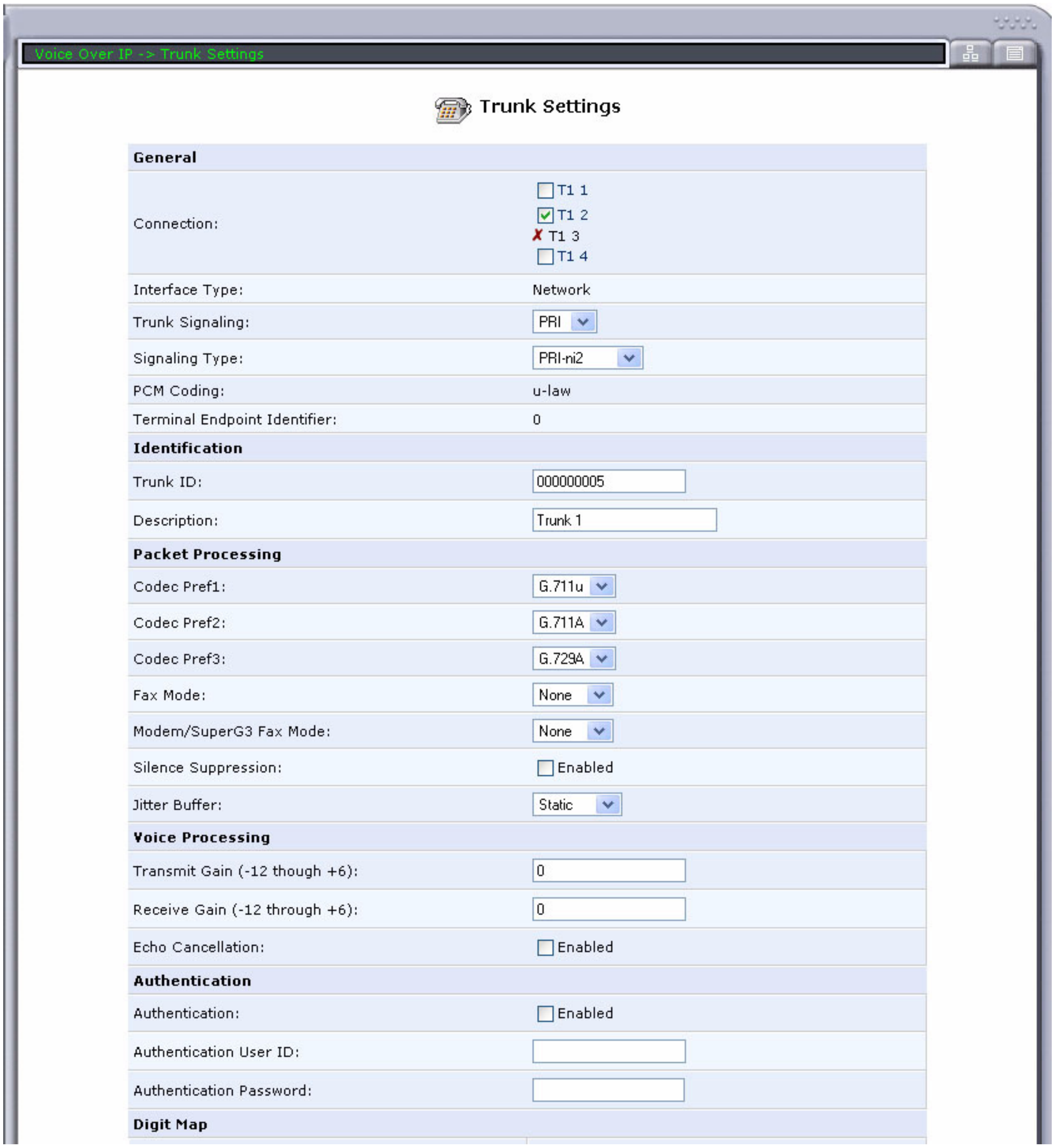


Trunk	Description	Connection Type	Interface Type	Trunk Signaling	Action
000000005	Trunk 1	T1	Network	PRI	

Configuring Trunk Settings

To configure the trunk:

1. Select the **Voice Over IP/Trunk Settings** tab.
2. Select the **Trunk**. The Trunk Settings window appears. See the following table for field definitions.



Voice Over IP -> Trunk Settings

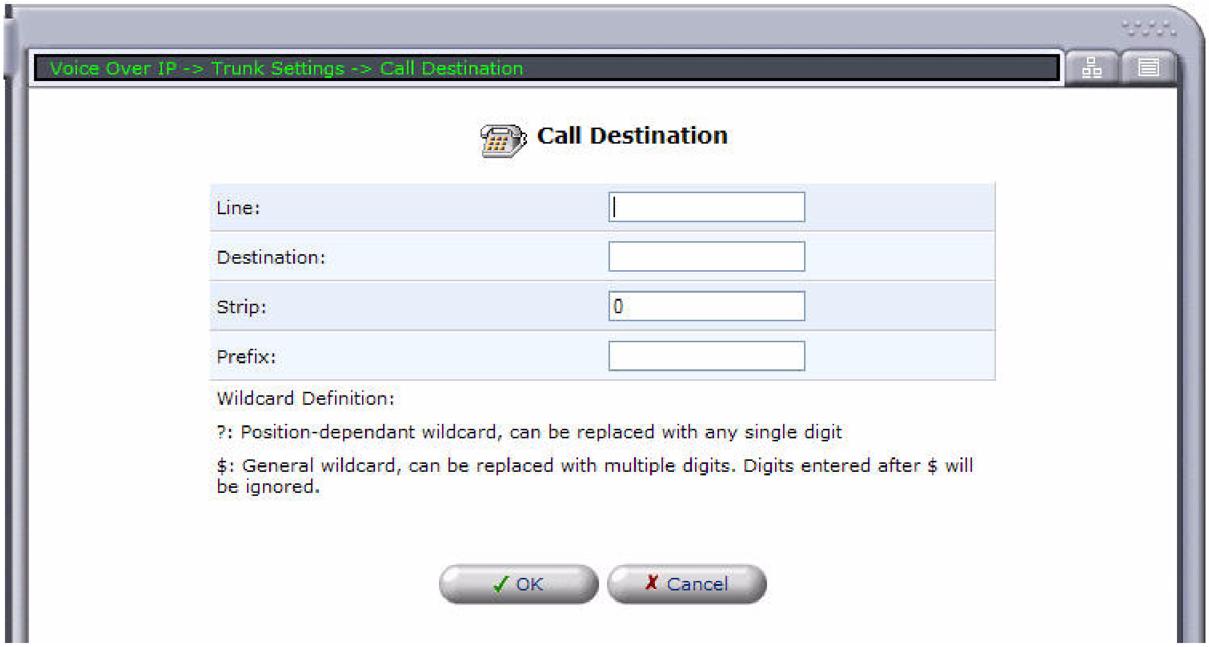
Trunk Settings

General	
Connection:	□ T1 1 ☑ T1 2 ✗ T1 3 □ T1 4
Interface Type:	Network
Trunk Signaling:	PRI
Signaling Type:	PRI-ni2
PCM Coding:	u-law
Terminal Endpoint Identifier:	0
Identification	
Trunk ID:	000000005
Description:	Trunk 1
Packet Processing	
Codec Pref1:	G.711u
Codec Pref2:	G.711A
Codec Pref3:	G.729A
Fax Mode:	None
Modem/SuperG3 Fax Mode:	None
Silence Suppression:	□ Enabled
Jitter Buffer:	Static
Voice Processing	
Transmit Gain (-12 though +6):	0
Receive Gain (-12 through +6):	0
Echo Cancellation:	□ Enabled
Authentication	
Authentication:	□ Enabled
Authentication User ID:	
Authentication Password:	
Digit Map	

Field	Definition
General	
Connection	**Adit 3500:** Connections are **T1 #1** through **T1 #4.** Select the checkbox for the T1 to apply the trunk settings to. **Note:** A red **X** indicates that the T1 is not available. **Adit MSR:** Connections are **LCC #1** through **LCC #8.** Select the checkbox for the LCC to apply the trunk settings to. **Note:** A red **X** indicates that the LCC is not available. **Note:** For the Adit MSR, when you select an LCC and apply it to the trunk, the cross-connect status is displayed below the link number. The status indications are: **No cross-connect** - No cross-connect has been made for the selected link. **Cross-connected to *x*** - A cross-connect with compatible protocol has been made. (*x* is the name of the cross-connected entity on the controller. For example, a:1:1-24.) **Incompatible CAS/PRI Protocol on *x*** - There is an incompatibility in signaling protocol or link selection between the controller and MSR card. (*x* is defined as above.) **Note:** When you select the connection's name, the **Channel Configuration** appears. See the *Channel Configuration on page 6-30.*
Interface Type	Displays the interface type (Network).
Trunk Signaling	Sets the signaling type of the trunk. **PRI** - Primary Rate Interface **CAS** - Channel Associated Signaling
Signaling Type	Sets the signaling type protocol on the trunk. **Note:** Hunt sequence of the PRI is a Round-Robin type, and is not configurable. **If PRI is selected above:** **PRI-ni2** - The CCITT National ISDN 2 PRI standard. **PRI-4ess** - The class 4 US AT&T proprietary version of ISDN. **PRI-5ess** - The class 5 ISDN central office circuit switching system developed by AT&T. **PRI-dms100** - Digital central office switch (number 100) from Northern Telecom. **If CAS is selected above:** **EM Wink Start** - E&M Wink Start. **EM Immediate Start** - E&M Immediate Start. **EM Delay Wink Start** - E&M Delay Wink Start.
PCM Coding	Displays the defined Pulse Code Modulation.
Terminal Endpoint Identifier	Displays the Terminal Endpoint Identifier for the trunk.

Field	Definition (Continued)
Identification	
Trunk ID	Display/edit the Trunk ID. A default ID is assigned. The Trunk ID can have up to 20 characters.
Description	Display/edit a Trunk Description. By default they are named Trunk *n*.
Packet Processing	
Codec Pref1 **Codec Pref2** **Codec Pref3**	Define the preference order of the Codecs. **G.711u** - G.711 mu-law **G.711A** - G.711 A-law **G.729A** - G.729 A-law **None**
Fax Mode	**None** - A Fax call will be treated as a normal voice call. Default. **Bypass** - Will cause the line to transmit in G.711 mode, with silence suppression disabled, on detection of Fax tone. **T38** - The Adit MSR will support T.38 in a future release.
Modem/SuperG3 Fax Mode	**None** - A Modem call will be treated as a normal voice call. Default. **Bypass** - Will cause the line to transmit in G.711 mode, with silence suppression disabled, on detection of Modem tone.
Silence Suppression	Enable or disable silence suppression for voice calls, for one or more voice channels.
Jitter Buffer	**Static** - Maintain a static average delay, = 2x the packet time (Default) **Dynamic** - Perform dynamic delay adjustment to minimize delay
Voice Processing	
Transmit Gain	Set the gain on the transmit side voice path for the specified voice channel(s). Range is -12 to 6, with a default of 0.
Receive Gain	Set gain on the receive side voice path for the specified voice channel(s). Range is -12 to 6, with a default of 0.
Echo Cancellation	Check to enable Echo Cancellation on this trunk.
Calling Features	
Block Outgoing Caller ID	Enables/disables blocking of Caller ID on SIP calls made from this trunk.
Authentication	
Authentication	Check to enable authentication on this trunk.
Authentication User ID	Enter User ID.
Authentication Password	Enter Authentication Password.

Field	Definition (Continued)
Digit Map	
Per Trunk Digit Map	**Disabled** - Use the phone book, maximum digits, or dialing timeout to determine end of dialing. Default. **Default Digit Map** - Pass dialed number as a complete number for routing to the phone book, or to the proxy if there are no9 phone book entries. **Custom Digit Map** - Process as for the default digit map. **Note:** The field name is a link to the Digit Map configuration window. See *Configuring the Digit Map on page 6-6*.
New Entry - See **Call Destination** window below.	
Line	Number (1-30) for the dial pattern.
Destination	Identifies the destination of the incoming phone call.
Strip	The number of digits to be stripped off from the left-most digits in the phone number. Possible usages include stripping off the area code, or the 3-digit office prefix. Range is 0 - 7, with a default of 0.
Prefix	The digits or a name to be added to the phone number after the stripping process has been applied. This field is empty by default.



Voice Over IP -> Trunk Settings -> Call Destination

Call Destination

Line:	
Destination:	
Strip:	0
Prefix:	

Wildcard Definition:

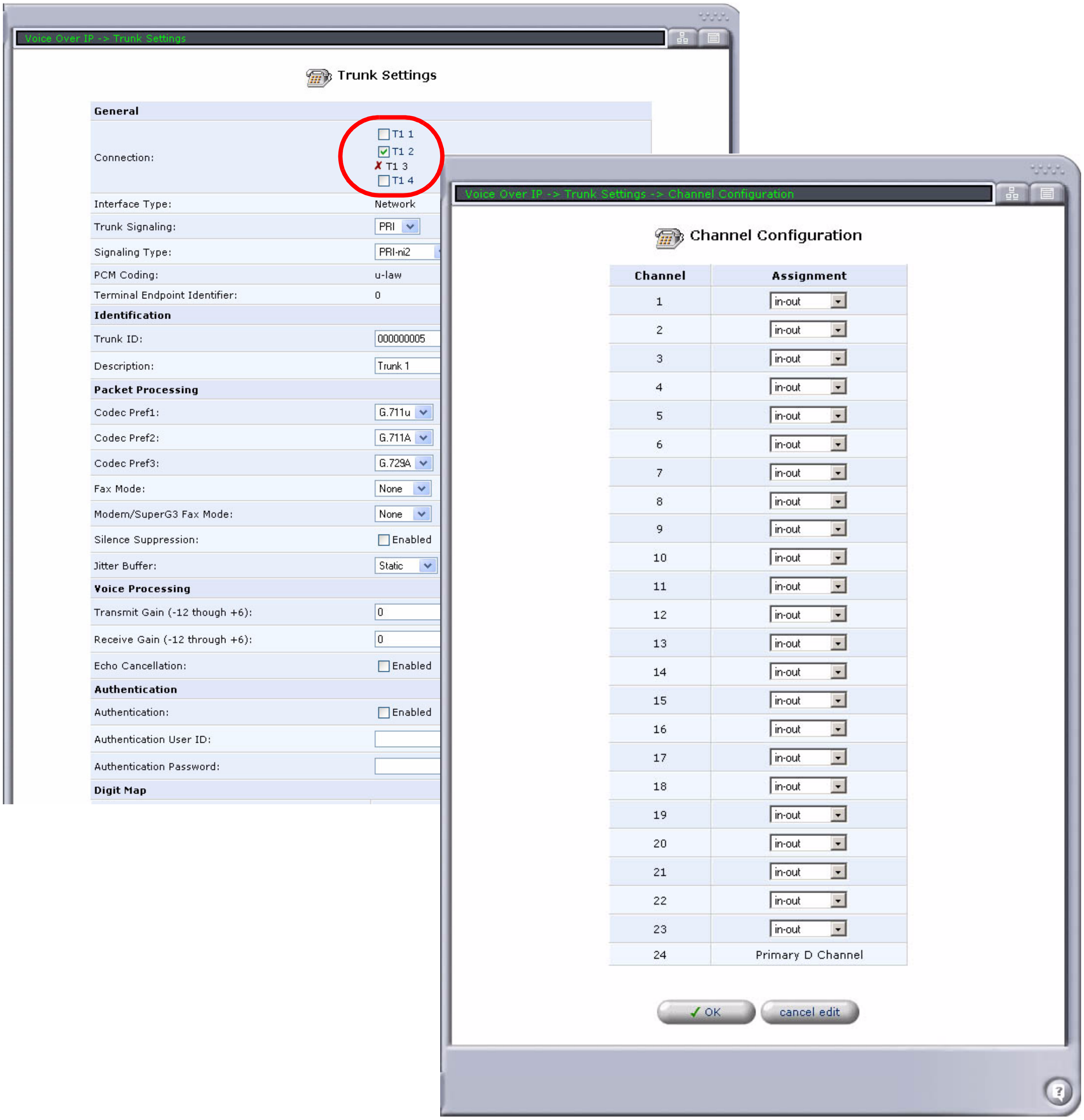
?: Position-dependant wildcard, can be replaced with any single digit

$: General wildcard, can be replaced with multiple digits. Digits entered after $ will be ignored.

Channel Configuration

The **Channel Configuration** window displays the communication assignment for each channel in the trunk. For the Adit 3500, you can change the channel assignments at this window. For the Adit MSR, the assignments are fixed.

To view the **Channel Configuration** window, select one of the connections listed in the **Connection** field on the the **Voice Over IP/Trunk Settings** tab. (Adit 3500 shown below.)



Voice Over IP -> Trunk Settings

Trunk Settings

General	
Connection:	□ T1 1 ☑ T1 2 ✗ T1 3 □ T1 4
Interface Type:	Network
Trunk Signaling:	PRI
Signaling Type:	PRI-ni2
PCM Coding:	u-law
Terminal Endpoint Identifier:	0
Identification	
Trunk ID:	000000005
Description:	Trunk 1
Packet Processing	
Codec Pref1:	G.711u
Codec Pref2:	G.711A
Codec Pref3:	G.729A
Fax Mode:	None
Modem/SuperG3 Fax Mode:	None
Silence Suppression:	□ Enabled
Jitter Buffer:	Static
Voice Processing	
Transmit Gain (-12 though +6):	0
Receive Gain (-12 through +6):	0
Echo Cancellation:	□ Enabled
Authentication	
Authentication:	□ Enabled
Authentication User ID:	
Authentication Password:	
Digit Map	

Voice Over IP -> Trunk Settings -> Channel Configuration

Channel Configuration

Channel	Assignment
1	in-out
2	in-out
3	in-out
4	in-out
5	in-out
6	in-out
7	in-out
8	in-out
9	in-out
10	in-out
11	in-out
12	in-out
13	in-out
14	in-out
15	in-out
16	in-out
17	in-out
18	in-out
19	in-out
20	in-out
21	in-out
22	in-out
23	in-out
24	Primary D Channel

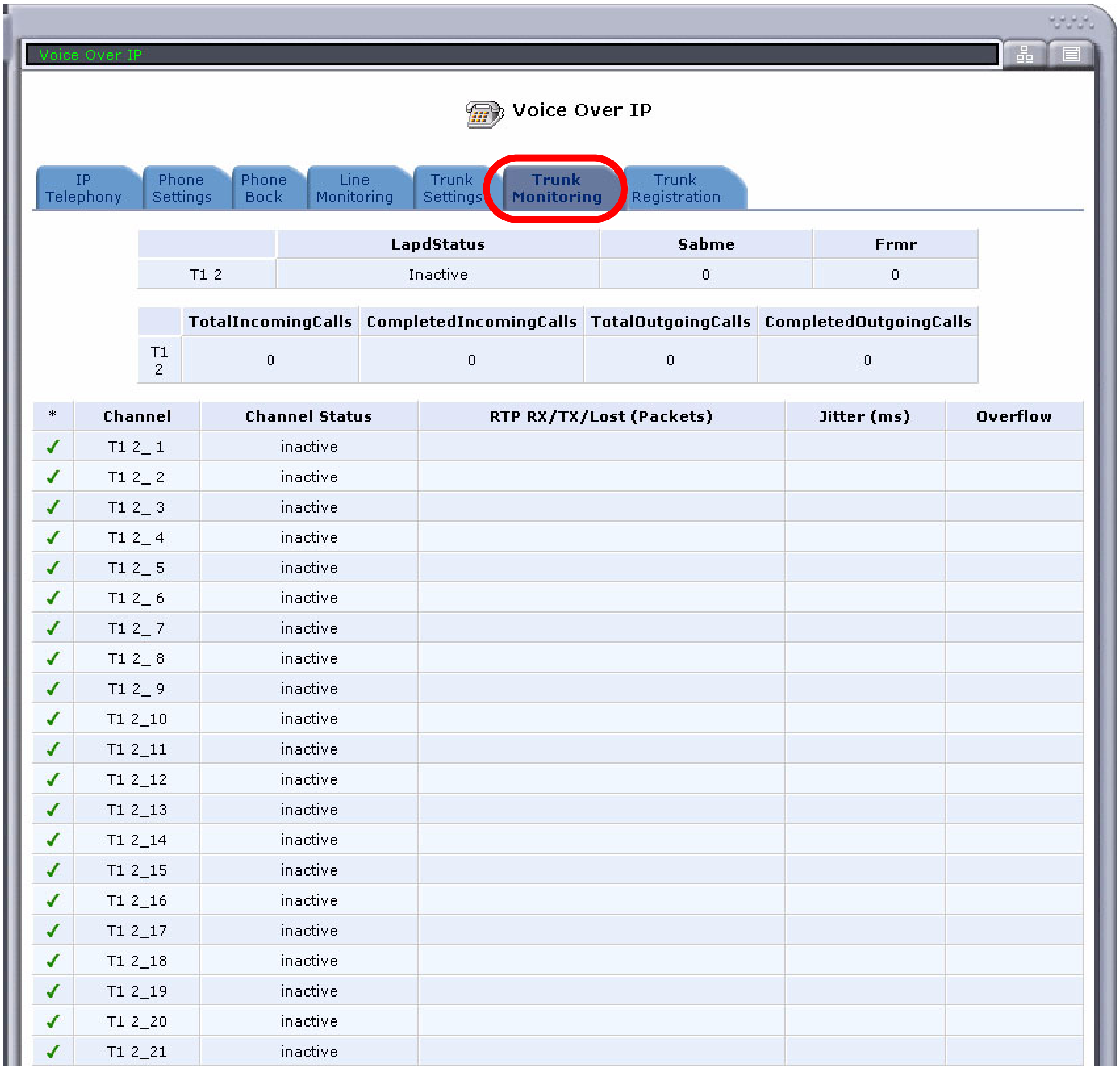
Field	Definition
Assignment	**in-out** - Allows comminution in both directions. Default. **in** - Allows communication in the IN direction only. **out** - Allows communication in the OUT direction only. **unassigned** - Puts the channel out-of-service (down).

Trunk Monitoring

NOTE: The **Trunk Monitoring** tab is only available on the Adit 3500 and Adit MSR.

The Trunk Monitoring window displays current status and statistics for trunk channels.

Adit 3500

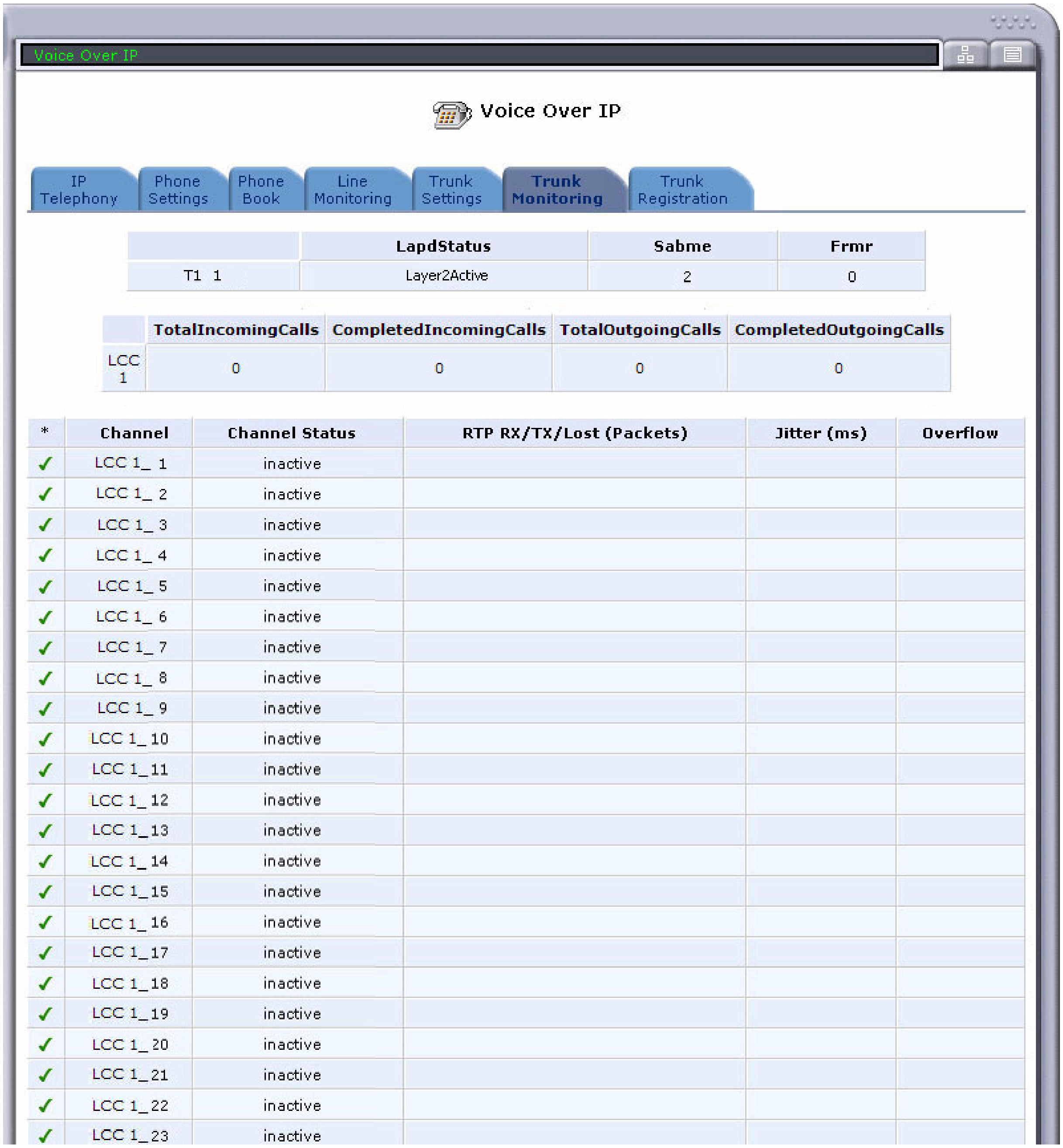


	LapdStatus	Sabme	Frmr
T1 2	Inactive	0	0

	TotalIncomingCalls	CompletedIncomingCalls	TotalOutgoingCalls	CompletedOutgoingCalls
T1 2	0	0	0	0

*	Channel	Channel Status	RTP RX/TX/Lost (Packets)	Jitter (ms)	Overflow
✓	T1 2_ 1	inactive			
✓	T1 2_ 2	inactive			
✓	T1 2_ 3	inactive			
✓	T1 2_ 4	inactive			
✓	T1 2_ 5	inactive			
✓	T1 2_ 6	inactive			
✓	T1 2_ 7	inactive			
✓	T1 2_ 8	inactive			
✓	T1 2_ 9	inactive			
✓	T1 2_10	inactive			
✓	T1 2_11	inactive			
✓	T1 2_12	inactive			
✓	T1 2_13	inactive			
✓	T1 2_14	inactive			
✓	T1 2_15	inactive			
✓	T1 2_16	inactive			
✓	T1 2_17	inactive			
✓	T1 2_18	inactive			
✓	T1 2_19	inactive			
✓	T1 2_20	inactive			
✓	T1 2_21	inactive			

Adit MSR



	LapdStatus	Sabme	Frmr
T1 1	Layer2Active	2	0

	TotalIncomingCalls	CompletedIncomingCalls	TotalOutgoingCalls	CompletedOutgoingCalls
LCC 1	0	0	0	0

*	Channel	Channel Status	RTP RX/TX/Lost (Packets)	Jitter (ms)	Overflow
✓	LCC 1_ 1	inactive			
✓	LCC 1_ 2	inactive			
✓	LCC 1_ 3	inactive			
✓	LCC 1_ 4	inactive			
✓	LCC 1_ 5	inactive			
✓	LCC 1_ 6	inactive			
✓	LCC 1_ 7	inactive			
✓	LCC 1_ 8	inactive			
✓	LCC 1_ 9	inactive			
✓	LCC 1_10	inactive			
✓	LCC 1_11	inactive			
✓	LCC 1_12	inactive			
✓	LCC 1_13	inactive			
✓	LCC 1_14	inactive			
✓	LCC 1_15	inactive			
✓	LCC 1_16	inactive			
✓	LCC 1_17	inactive			
✓	LCC 1_18	inactive			
✓	LCC 1_19	inactive			
✓	LCC 1_20	inactive			
✓	LCC 1_21	inactive			
✓	LCC 1_22	inactive			
✓	LCC 1_23	inactive			

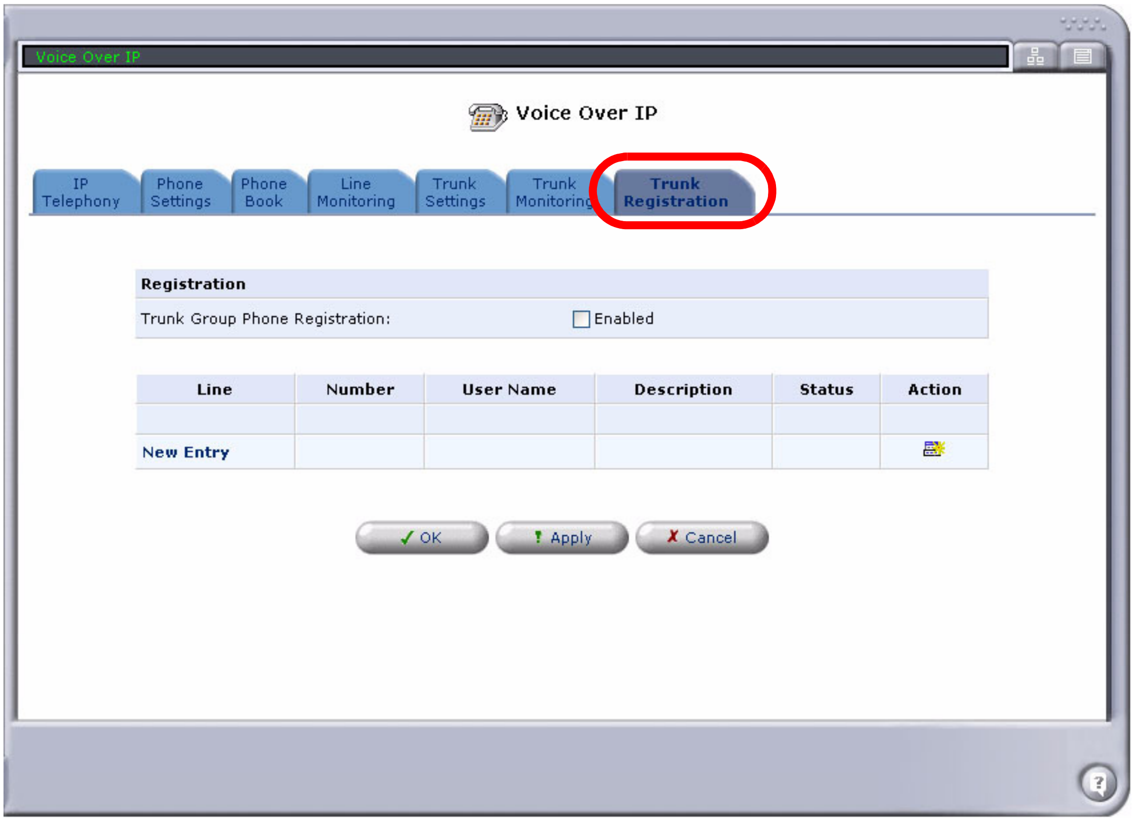
The following table defines the fields displayed in the **Trunk Monitoring** window:

Field	Definition
PRI Interface - For each PRI interface the following is displayed:	
LapdStatus	The operational status of the LAPD (Link Access Procedure on the D channel) status. (Inactive, Layer1Active, Layer2Active.
Sabme	The number of peer SABME (Asynchronous Balanced Mode Extended) frames received on this interface.
Frmr	The number of LAPD FRMR (Frame Reject status) response frames received. This is the number of framing errors on this interface.
TotalIncomingCalls	Displays the number of Incoming Calls
CompletedIncomingCalls	Displays the number of Incoming Connected Calls
TotalOutgoingCalls	Displays the number of Outgoing Calls
CompletedOutgoingCalls	Displays the number of Outgoing Connected Calls
Channel	The ID of the PRI (bearer) channel.
Channel Status	Displays the channel (bearer) status - unassigned, inactive, idle, busy.
RTP RX/TX/Lost (Packets)	Packets received/transmitted/dropped.
Jitter (ms)	Milliseconds of Jitter incurred on the call.
Overflow	Displays the overflow when there are too many packets to buffer.

Trunk Registration

NOTE: The **Trunk Registration** tab is only available on the Adit 3500 and Adit MSR.

The **Trunk Registration** tab displays all configured PBX phone lines.



Registration

Trunk Group Phone Registration: □ Enabled

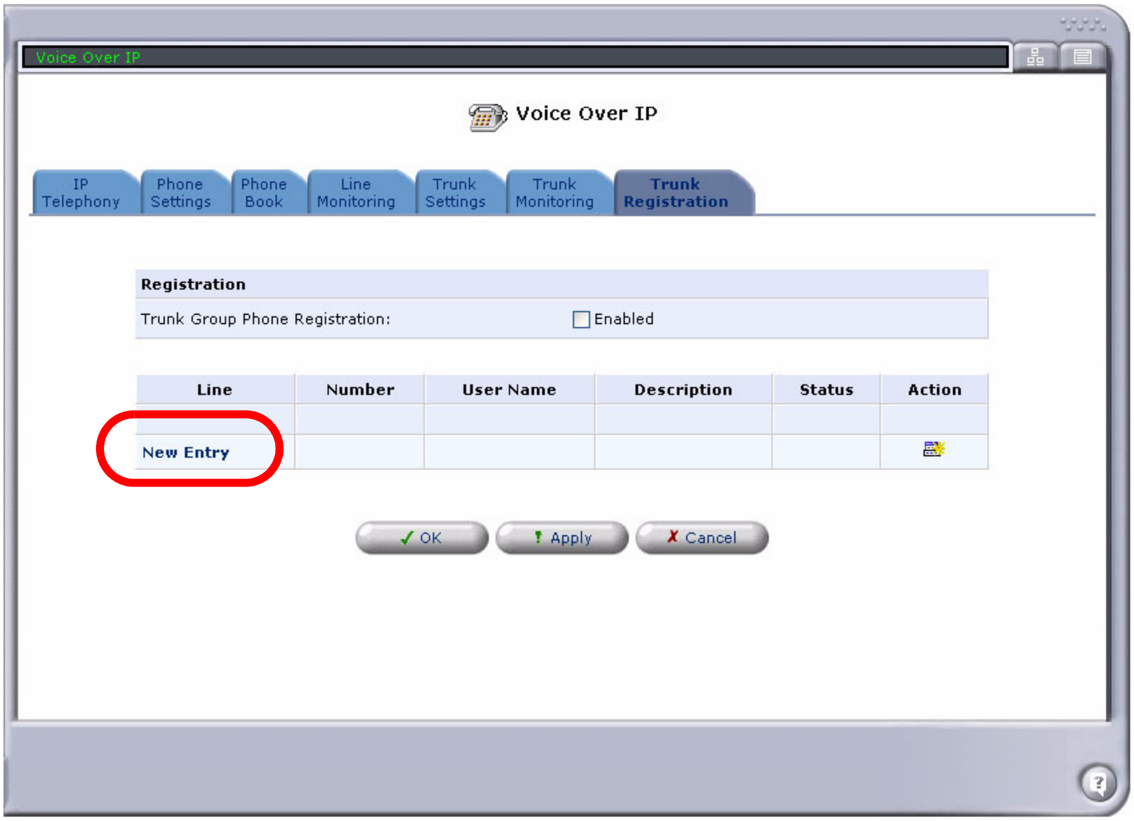
Line	Number	User Name	Description	Status	Action
New Entry					

Field	Definition
Trunk Group Phone Registration	Enable/disable the trunk group phone registration feature.
Line	Displays the line number. The checkbox allows this line to be disabled (unchecked) without having to delete the configuration.
Number	Displays the defined phone number.
User Name	Displays the defined user name.
Description	Displays the description.
Status	Displays the current status.
Action	The two icons allow the user to edit or delete the line.
New Entry	Opens the **Add PBX Phone Line** window, which is used to configure the lines that are displayed on this table.

Adding a PBX Phone Line

To add a new PBX phone line:

1. Select **New Entry** from the **Voice Over IP/Trunk Registration** window.

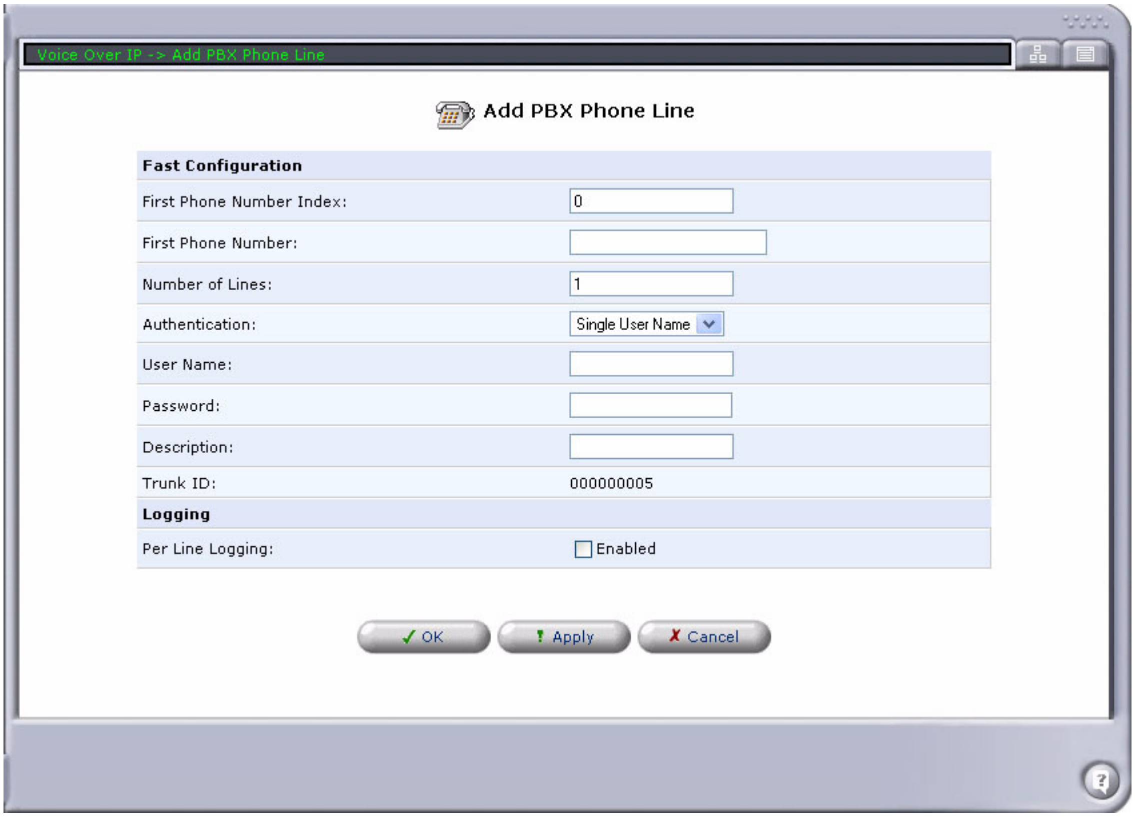


Registration

Trunk Group Phone Registration: □ Enabled

Line	Number	User Name	Description	Status	Action
New Entry					

2. Enter the PBX line information. See the following table for field definitions.



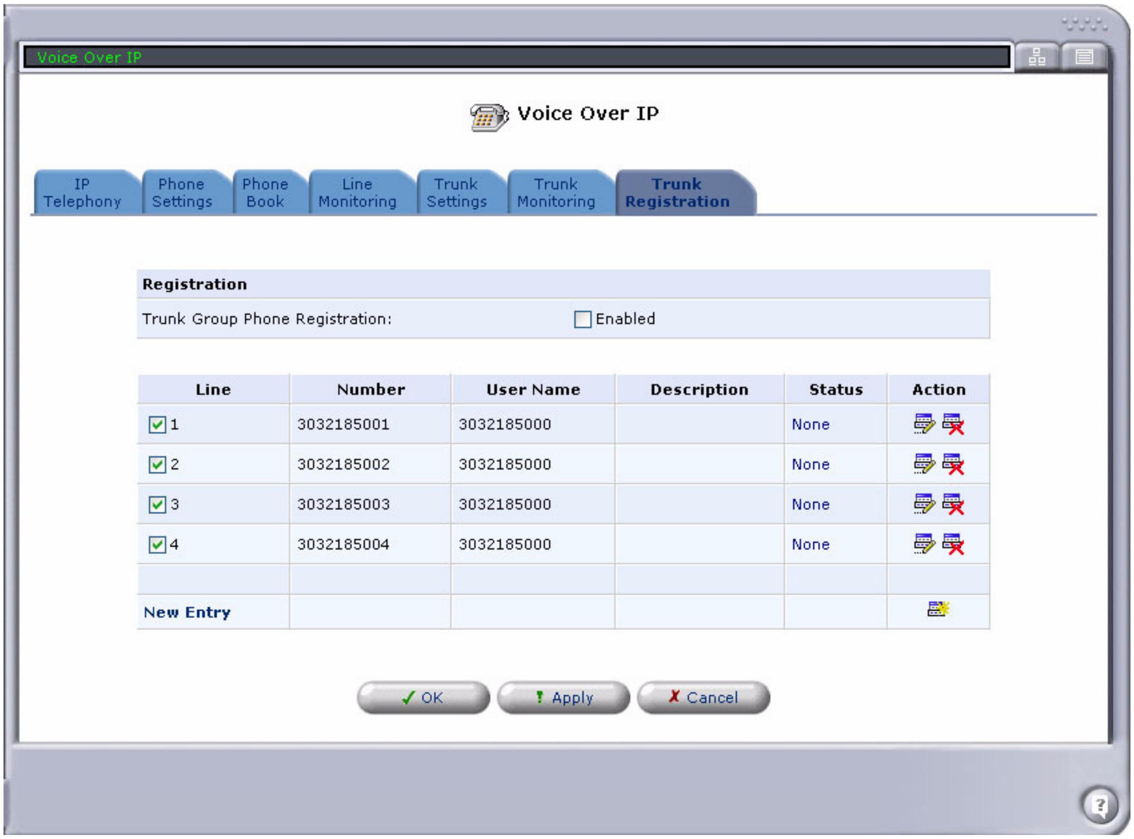
Voice Over IP -> Add PBX Phone Line

Add PBX Phone Line

Fast Configuration	
First Phone Number Index:	0
First Phone Number:	
Number of Lines:	1
Authentication:	Single User Name
User Name:	
Password:	
Description:	
Trunk ID:	000000005
Logging	
Per Line Logging:	□ Enabled

Field	Definition
Fast Configuration	
First Phone Number Index	Enter an index number for the phone number. If a number entered is already listed, it will be overwritten. If the number is left at "0" then the next available index number will be selected.
First Phone Number	Enter a PBX phone number for this line.
Number of Lines	Enter the number of lines to enter (they will be sequential following the number entered above).
Authentication	**Single User Name** - Authentication will be with the user name. **Phone Number** - Authentication will be with the phone number entered.
User Name	Enter a User Name, with a maximum of 65 characters.
Password	Enter a password associated with the User Name, with a maximum of 64 characters.
Description	Enter a description, with a maximum of 20 characters. **Note:** This is not a required field.
Trunk ID	Displays the Trunk ID.
Logging	
Per Line Logging	The checkbox enables (checked) or disables (unchecked) logging for each line.

3. Select **OK** to enter the number and return to the **Trunk Registration** window.



Registration

Trunk Group Phone Registration: □ Enabled

Line	Number	User Name	Description	Status	Action
☑ 1	3032185001	3032185000		None	
☑ 2	3032185002	3032185000		None	
☑ 3	3032185003	3032185000		None	
☑ 4	3032185004	3032185000		None	
New Entry					

GLOSSARY

AMI	Automatic Mark Inversion
ARP	Address Resolution Protocol
B8ZS	Bipolar with 8 Zero Substitution
BIT	Binary Digit
BPS	Bits Per Second
BPV	Bipolar Violation
CA	Certificate Authority
CAS	Channel Associated Signaling
CCS	Common Channel Signaling
CHAP	Challenge Handshake Authentication Protocol
CID	Caller ID
CIDR	Classless Inter-Domain Routing
CLASS	Custom Local Area Signaling Service
CLEI	Common Language Equipment Identification
CLI	Command Line Interface
CO	Central Office
CPD	Calling Party Disconnect
CPE	Customer Provided Equipment
CRC	Cyclic Redundancy Check
CRV	Call Reference Value
CSU	Channel Service Unit
dB	decibel
DCS	Digital Signal Processor
DDNS	Dynamic Domain Name System
DDS	Digital Data Service

DLC	Digital Loop Carrier
DLCI	Data Link Connection Identifier
DMZ	Demilitarized Zone
DNS	Domain Naming System
DS0	Digital Signal Level Zero (64 kbps) (1 voice channel)
DS1	Digital Signal Level 1 (1.544 Mbps)
DSU	Digital Service Unit/Data service Unit
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
ES	Errored Seconds
ESF	Extended Superframe
FDL	Facilities Data Link
FXS	Foreign Exchange Station
GS	Ground Start
HDB3	High Density Bipolar 3
IP	Internet Protocol
IPX	Internet Packet eXchange
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LAPD	Link Access Procedure on the D channel status
LBO	Line Build Out
LLC	Logical Link Control
LMI	Local Management Interface
LS	Loop Start
LULT	Line Unit Line Termination
Mbps	Million Bits Per Second
MGCP	Media Gateway Control Protocol
MLPPP	Multilink PPP

MPPE	Microsoft Point-to-Point Encryption
MS-CHAP	Microsoft CHAP
MVEC	Majority Vote Error Correction
NAT	Network Address Translation
NCS	Network-based Call Signaling
NEBS	Network Equipment Building Standards
NRZ	Non-Return to Zero
NSE	Named Service Event
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAP	Password Authentication Protocol
PHY	Physical specifications
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In Service
SABME	Set Asynchronous Balanced Mode Extended
SDP	Session Description Protocol
SIP	Session Initiation Protocol
STP	Spanning Tree Protocol
T1	Trunk Level 1 (1.544 Mbps)
TDM	Time Division Multiplex
TEI	Terminal Endpoint Identifier
TFTP	Trivial File Transfer Protocol
TOS	Type of Service
UAC	User Agent Client

UAS	User Agent Server
VC	Virtual Channel
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WINS	Windows Internet Naming Service

10Base-T

The most widely installed Ethernet local area networks (LANs) use ordinary telephone twisted-pair wire. When used on Ethernet, this carrier medium is known at 10BASE-T. 10BASE-T supports Ethernet's 10 Mbps transmission speed.

100Base-TX

Also called "Fast Ethernet", it is a 100 Mbps version of Ethernet. 100Base-T transmits at 100 Mbps rather than 10 Mbps. Like regular Ethernet, Fast Ethernet is a shared media LAN. All nodes share the 100 Mbps bandwidth. 100Base-TX uses two pairs of Category 5 cabling, one pair for transmission, one pair for receiving.

Address Resolution Protocol (ARP)

An internet protocol used to map dynamic internet addresses to physical addresses on Local Area Networks.

Alternate Mark Inversion (AMI)

The line-coding format in T1 transmission systems whereby successive ones (marks) are alternately inverted (sent by polarity opposite that of the preceding mark).

analog

The telephone transmission of voice, video or image. Telephone transmission and/or switching that is not digital.

Asynchronous Transfer Mode (ATM)

Very high speed transmission technology. ATM is a high bandwidth, low-delay, connection-oriented, packet-like switching and multiplexijng technique. Usable capacity is segmented into 53-byte fixed-size cells, consisting of header and information fields, allocated to services on demand. The term "asynchronous" applies, as each cell is presented to the network on a "start-stop" basis - in other words, asynchronously.

authentication

The process of identifying an individual, usually based on a username and password combination, although the process can be many more steps. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Authentication in whatever form, is usually followed by authorization.

bandwidth

The width of a communications channel. Analog is typically measured in Hertz (cycles per second), a voice conversation is typically measured in bits per second.

Basic Rate Interface (BRI)

Basic Rate Interface (2b+d) in ISDN.

Bipolar 8-Zero Substitution

A coding scheme that maintains ones density.

bipolar violation

BPV. A violation is declared for AMI if two successive pulses have the same polarity.

bit

Contraction of the words "binary" and "digit".

Bit Error Rate

The number of erred bits divided by the total number of bits.

broadband

A technology that provides an extremely wide and fast bandwidth so that many people can simultaneously use the service. It is generally associated with multiple types of transmissions on the same connection such as voice, data, video and digital or analog information.

Central Office (CO) Where telephone companies terminate customer lines and locate switching equipment to interconnect those lines with other networks.

channel A generic term for a communications path on a given medium; multiplexing techniques allow providers to put multiple channels over a single medium.

Channel Associated Signaling (CAS) Carrying signaling information within the data channels of a T1 line (in band) rather than on a separate control channel. CAS signaling is also used to carry 911 emergency data such as telephone number and location information.

Channel Service Unit (CSU) The interface to the T1 line that terminates the local loop.

Classless Inter-Domain Routing CIDR is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme.

CLEI Codes Common Language Equipment Identifier codes, that are assigned by Bellcore to provide a standard method of identifying telecommunications equipment in a uniform, feature-oriented language.

CLI Command Line Interface

collision In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device impact and are damaged when they meet on the physical media.

command line The command line is where you enter MS-DOS commands.

compander Companding is the process of compressing the amplitude range of a signal for economical transmission and then expanding them back to their original form at the receiving end.

Demilitarized Zone (DMZ) A collection of computers that are shielded from both the trusted network and the untrusted network by packet-filtering routers and gateways.

Domain Naming System (DNS) DNS. A mechanism used in the Internet for translating names of host computers into addresses.

download To transfer data from a larger “host” system to a smaller “client” system's hard drive or other local storage device.

Dual Tone Multi-Frequency (DTMF) Dual Tone Multi-Frequency is a term describing push button or Touchtone dialing.

Dynamic Domain Name System (DDNS) Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Dynamic Host Configuration Protocol (DHCP) DHCP is a network configuration that allows maintenance to be performed from a central site rather than by end users.

Earth ground A wire conductor that terminates in the earth for electrical purposes. It is generally the negative side of the circuit and is most important in alternating current (AC) circuits. Chassis Ground is the general term used in direct current (DC) circuits.

Electro-magnetic Interference (EMI)

Equipment used in high speed data systems, including ATM, that generate and transmit many signals in the radio frequency portion of the electromagnetic spectrum. Interference to other equipment or radio services may result if sufficient power from these signals escape the equipment enclosures or transmission media. National and international regulatory agencies (FCC, CISPR, etc.) set limits for these emissions. Class A is for industrial use and Class B is for residential use.

Ethernet

Ethernet is a particular network topology and protocol, especially useful in LANs. It comes in various speeds and is often regarded as THE current technology for general network direct connection. The current connectivity is generally considered to be 10Base-T or 100Base-T, while the backbone, if one is used, is coaxial cable or Fiber optics. There is also a 1000Base-T for certain specialty copper joining situations.

Facilities Data Link (FDL)

FDL supports the communication of various network information in the form of in-service monitoring and diagnostics.

filter

An operating parameter used with routers that can be set to block the transfer of packets from one LAN to another.

firewall

Any of a number of security schemes that prevent unauthorized users from gaining access to a computer network and/or may monitor the transfer of information to and from the network.

frame

A fragment of data that is packaged into a frame format, which comprises a header, payload, and trailer.

Frame Reject (FRMR)

The FRMR response frame is sent to report the receiver of a frame cannot successfully process that frame and that the error condition is not correctable by sending the offending frame again.

Foreign Exchange

A Central Office trunk which has access to a distant central office. Dial Tone is returned from that distant Central Office, and a location can be reached in the area of the foreign Central Office by dialing a local number. This will provide easier access for customers in that area and calls may be made anywhere in the foreign exchange area for a flat rate.

Foreign Exchange Service

Foreign exchange (FX) service is a service that can be ordered from the telephone company that provides local telephone service from a central office which is outside (foreign to) the subscriber’s exchange area. Simply, a user can pick up the phone in one city and receive a dial tone in the foreign city. This kind of connection is provided by a type of trunk called foreign exchange (FX) trunk. FX trunk signaling can be provided over analog or T-1 links. Connecting POTS telephones to a computer telephony system via T-1 links requires a channel bank configured with FX type connections.

G.711

ITU-T Recommendation for an algorithm designed to transmit and receive A-law and mu-law PCM voice at digital bit rates of 48, 56, and 64 Kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.729

International Telecommunications Union’s standard voice algorithm (CS-ACELP) voice algorithm for the coding of encoding/decoding of speech at 8 Kbps using conjugate-structure, algebraic-code excited linear predictive methods. Described in the ITU-T standard in its G-series recommendations.

gateway
An entrance and exit into a communications network

Graphical User Interface (GUI)
GUI, pronounced “GOOEY”. A set of screen presentations and metaphors that utilize graphic elements such as icons in an attempt to make an operating system easier to use.

ground
A physical connection to the earth or other reference point.

ground start (GS)
A method of signaling on subscriber trunks in which one side of the two wire trunk (typically the ring conductor of Tip and Ring) is momentarily grounded to get dial tone.

hash algorithm
A one way function that takes an input message of arbitrary length and produces a fixed length digest. Adit uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes within our implementation of the IPSec framework.

High Density Bipolar 3
HDB3. A bipolar coding method that does not allow more than 3 consecutive zeros.

hop
Each individual short trip that packets make from router to router, as they are routed to their destination.

host
A computer that allows users to communicate with other host computers on a network.

impedance
The total opposition a circuit offers to the flow of alternating current. It is measured in ohms and the lower the ohmic value, the better the quality of the conductor

internet
“A network of networks,” the Internet supports FTP, WWW, Gopher, E-Mail, Telnet, and many other world-wide information transfer protocols and services. ISPs provide an effective interface with the Internet. The Internet itself is made up of thousands of LANs and WANs, all using TCP/IP to provide information services to millions of users. A worldwide network of networks that all use the TCP/IP communications protocol and share a common address space.

Internet Protocol (IP)
Internet Protocol, the method by which most Internet activity takes place. Members with access to TCP/IP through a SLIP or PPP connection can connect to many ISP services in this manner. As the name implies, it is a protocol for network activity. Most current networks support some sort of TCP or IP directly or indirectly.

IP address
A string of four numbers separated by periods (such as 111.22.3.144) used to represent a computer on the Internet. The format of the address is specified by the Internet Protocol in RFC 791. Each of the four number must be 255 or less; they may be 0.

IPSec
IPSec (IP Security) is a set of IP extensions developed by IETF to provide security services compatible with the existing IP standard (IPv.4) and also the upcoming one (IPv.6). In addition, IPSec can protect any protocol that runs on top of IP, for instance TCP, UDP, and ICMP. The IPSec provides cryptographic security services. These services allow for authentication, integrity, access control, and confidentiality. IPSec allows for the information exchanged between remote sites to be encrypted and verified. You can create encrypted tunnels (VPNs), or just do encryption between computers.

jitter
Interference on an analog line caused by a variation of a signal from its reference timing slots. Jitter can cause problems in the receipt of data and any subsequent processing of that data.

Local Area Network (LAN)
A short distance data communications network (typically within a building or campus) used to link together computers and peripheral devices under some form of standard control.

Line Build Out (LBO)
T1s require the last span to lose 15 - 22.5 dB, a selectable output attenuation is generally required of DTE equipment.

Line Coding Violation (LCV)
This parameter is a count of both BPVs and EXZs occurring over the accumulation period. An EXZ increments the LCV by one regardless of the length of the zero string.

Line Errored Seconds (LES)
A Line Errored Second is a second in which one or more CVs occurred OR one or more LOS defects.

Local Link Control (LLC)
A protocol developed by the IEEE 802.2 committee for data-link-level transmission control

Local Management Interface
A specification for the use of frame-relay products that define a method of exchanging status information between devices such as routers

loop start (LS)
A method of demanding dial tone from the central office by completing an electrical pathway between the outbound and return conductors of a telephone line. Loop start is employed by single-line telephone instruments, for example

loopback
A diagnostic test in which a signal is transmitted across a medium while the sending device waits for its return.

MAC Address
The address for a device as it is identified at the Media Access Control layer in the network architecture

Management Information Base (MIB)
A data base of objects, with attributes and values, representing the manageable components of a network device. Used in SNMP. There are industry standardized MIBs and proprietary MIBs

mapping
In network operations, the logical association of one set of values, such as addresses on one network, with quantities or values of another set, such as devices on another network.

Media Access Control (MAC)
The lower of the two sub-layers of the data link layer defined by the IEEE. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used. The MAC contains the standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE.

Media Gateway Control Protocol (MGCP)
MGCP. A control and signal standard for the conversion of audio signals carried on telephone circuits (PSTN) to data packets carried over the Internet or other packet networks.

Microsoft CHAP
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension to RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

Multilink PPP (MLPPP)

MultiLink PPP. An extension to the point-to-point protocol that enables two channels to be linked together to double the throughput. It is used for ISDN transmission and channel bonding

Microsoft Point-to-Point Encryption (MPPE)

A 128-bit key or 40-bit key encryption algorithm using RSA RC4. MPPE provides for packet confidentiality between the remote access client and the remote access or tunnel server and is useful where IP security (IPSec) is not available. MPPE 40-bit keys are used to satisfy current North American export restrictions. MPPE is compatible with Network Address Translation.

modem

MOdulator-DEModulator, a device that takes digital computer signal, converts it to analog, and sends it across the phone line. Another modem on the reverse does the exact opposite action. Modems transfer data at different speeds or rates, called baud.

multiplexer

Electronic equipment which allows two or more signals to pass over one communications circuit. The circuit may be analog or digital

MUX

See multiplexer

NetBIOS

Network Basic Input/Output System.NetBIOS is a program that allows applications on different computers to communicate within a Local Area Network (LAN).

network

A set of computers linked to one another for data sharing, or the link itself.

Network Time Protocol (NTP)

Network Time Protocol, developed to maintain a common sense of time among Internet hosts around the world. Many systems on the Internet run NTP, and have the same time (relative to Greenwich Mean Time).

Non-Return to Zero (NRZ)

A binary encoding scheme in which ones and zeros are represented by opposite and alternating high and low voltages and where there is no return to a zero (reference) voltage between encoded bits.

Open Shortest Path First (OSPF)

Short for Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm.

Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography).

The advantage of shortest path first algorithms is that they results in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (when routers continuously increment the hop count to a particular network). This makes for a stable network.
Note: OSPF Version 2 is defined in RFC 1583. It is rapidly replacing RIP on the Internet.

packet

A packet consists of the data to be transmitted and certain control information.

PAP

Password Authentication Protocol

PAT

Port Address Translation

PHY PHY as in physical specifications. OSI Physical Layer, which provides for transmission of cells over a physical medium connecting two ATM devices.

ping Packet InterNet Grouper. PING is a program used to test whether a particular network destination on the Internet is online (i.e. working) by repeatedly bouncing a "signal" off a specified address and seeing how long that signal takes to complete the round trip. No return signal - site is down or unreachable. Portion is returned - trouble with the connection.

PLAR Private Line, Automatic Ringdown. A leased voice circuit that connects two single instruments together. When either handset is lifted, the other instrument automatically rings.

PPP Point-to-Point Protocol. is used for establishing a point-to-point link that provides a single, preestablished WAN communications path from the customer premises, through a carrier network (the telephone company), to a remote network

PPPoT1 Point-to-Point over T1.

PRACK Provisionable acknowledgement.

Primary Rate Interface (PRI) The ISDN equivalent of a T1. The Primary Rate Interface (delivered to the customer's premise) provides 23B+D (N.America) or 30B+D (Europe) running at 1.544 Mb/sec and 2.048 Mb/sec, respectively.

protocol Procedure or set of rules.

PVC Permanent Virtual Circuit. A PVC is a permanent channel connection between two ATM devices. PVC's allow network transmissions to be started without having to first establish a connection with the end point ATM device. When a PVC is constructed, the end points of the connection will agree upon a path in which data will travel, and therefore agree upon the route that data will travel to reach its destination.

Quality of Service (QoS) The measure of the telephone service quality provided to a subscriber.

RADIUS Remote Authentication Dial-In Service. RADIUS is a client/server-based authentication software system. The software supports remote access applications, allowing an organization to maintain user profiles in a centralized database residing on an authentication server which can be shared by multiple remote access servers.

robbed bit A type of analog signaling that will occasionally steal information bits used for circuit signaling coding.

router A computer or internet working device that directs traffic and moves packets between networks. A hardware architecture used in LANs, MANs, WANs, the Internet and Intranets. A device that connects any number of LANs. Routers use headers and a forwarding table to determine where packets go, and they use ICMP to communicate with each other and configure the best route between any two hosts.

Router Information Protocol (RIP)

RIP is based on distance vector algorithms that measure the shortest path between two points on a network, based on the addresses of the originating and destination devices. The shortest path is determined by the number of hops between those points. Each router maintains a routing table, or routing database, of known addresses and routes; each router periodically broadcasts the contents of its table to neighboring routers in order that the entire network can maintain a synchronized database.

Router Information Protocol Version 1 (RIPv1)

Original version of RIP. This is a classful routing protocol, it does not have the ability to transmit the subnet mask within its updates. RIP v1 imposes the subnet mask on the inbound interface and this is normally defined by the engineer. Learned routes are entered into the routing table with their natural mask. As a result there can be a great waste of internet host addresses.

Router Information Protocol Version 2 (RIPv2)

Second version of RIP, additional to Version 1, enables the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supports subnet masks, a critical feature that is not available in RIP (v1).

SAP

Service Access Point.

Session Initiation Protocol (SIP)

SIP is the emerging standard for setting up telephone call, multimedia conferencing, instant messaging and other types of real-time communication on the internet.

signal

A generated electrical impulse that is a change in voltage to trigger an event.

Simple Network Management Protocol (SNMP)

SNMP is the most common method by which network managements applications can query a management agent using a supported MIB (Management Information Base). SNMP operates at the OSI application layer.

spanning tree

Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations.

SRV

SRV is an resource record that specifies the locations of servers.

subnet mask

32-bit quantity indicating which bits in an IP address identify the physical network

T1

Trunk Level 1. A digital transmission link with a total signaling speed of 1.544 Mbps. T-1 is a standard for the digital transmission in North America.

telnet

An Internet standard protocol that enables a computer to function as a terminal working from a remote computer

TDM

Time Division Multiplex. A technique for transmitting a number of separate data, voice and/or video signals simultaneously over one communications medium by quickly interleaving a piece of each signal one after another.

Terminal Endpoint Identifier (TEI)

Up to eight devices can be connected to one ISDN BRI (or PRI) line. The TEI defines, for a given message, which of the eight devices is communicating with the Central Office switch. In general, more than one of the eight may be communicating.

TFTP

Trivial File Transfer Protocol.

ticks	The distance between two networks, measured in time increments. Ticks may be used to designate primary and secondary routes to the same network.
traffic	The load of packets carried by a network or portion of a network. Heavy traffic slows down the response time of the individual packets.
trunk	A communication line between two switching systems.
tunneling	To provide a secure, temporary path over the Internet.
User Agent Client (UAC)	One of the two types of User Agents in SIP. UAC initiates a request that is sent to a UAS.
User Agent Server (UAS)	One of the two types of User Agents in SIP. UAS receives a request from a UAC and returns.
V.90	The standard for full-duplex modems sending and receiving data across phone lines at up to 56,600 bps, approved by the International Telecommunication Union (ITU) in February, 1998.
Virtual Private Network (VPN)	A software defined network offering the appearance, functionality and usefulness of a dedicated private network, at a price savings.
VC MUX	Virtual Channel Multiplexer
Wide Area Network (WAN)	A private long distance network that uses leased lines to connect computers or LANs. A wide area network is a linking of computers not physically attached through conventional network connectivity. Usually the WAN connection is a dedicated or high grade dial up phone link. It is often done with T1 or T3 connections but can also be through satellite or other technologies.
WINS	Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer.
Virtual Connection (VC)	A connection between two hosts in a packet-switching network. In this case, the two hosts can communicate as though they have a dedicated connection even though the packets might actually travel very different routes before arriving at their destination.
Virtual Local Area Network (VLAN)	A VLAN consists of a network of computers that behave as if connected to the same wire, though they may actually be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible.

INDEX